

Release Notes: Junos[®] OS Release 12.3X48-D105 for the SRX Series

Release 12.3X48-D105
4 August 2020
Revision 1

Contents	Introduction 12
	New and Changed Features 12
	Release 12.3X48-D105 Software Features 13
	Release 12.3X48-D100 Software Features 13
	Release 12.3X48-D95 Software Features 13
	Release 12.3X48-D90 Software Features 13
	Release 12.3X48-D85 Software Features 14
	Release 12.3X48-D80 Software Features 14
	Application Security 14
	Release 12.3X48-D75 Software Features 14
	Release 12.3X48-D70 Software Features 14
	Release 12.3X48-D65 Software Features 15
	Ethernet Switching 15
	Interfaces and Routing 15
	Release 12.3X48-D60 Software Features 16
	High Availability 16
	Network Management and Monitoring 16
	Release 12.3X48-D55 Software Features 16
	Flow-Based and Packet-Based Processing 16
	Release 12.3X48-D45 Software Features 18
	Unified Threat Management (UTM) 18

Release 12.3X48-D40 Software Features	18
Dynamic Host Configuration Protocol (DHCP)	18
Network Address Translation (NAT)	18
Platform and Infrastructure	18
Release 12.3X48-D35 Hardware Features	19
Wireless WAN	19
Release 12.3X48-D35 Software Features	19
Interfaces	19
Unified Threat Management (UTM)	19
Release 12.3X48-D30 Software Features	20
Authentication and Access Control	20
Flow-Based and Packet-Based Processing	21
VPNs	21
Release 12.3X48-D25 Software Features	23
Application Layer Gateways (ALGs)	23
IP Monitoring	23
Network Address Translation (NAT)	23
System Logging	24
Unified Threat Management (UTM)	24
Release 12.3X48-D20 Software Features	25
Interfaces	25
Screens	25
Security Policies	25
VPNs	25
Release 12.3X48-D15 Software Features	26
Application Layer Gateways (ALGs)	26
Intrusion Detection Prevention (IDP)	27
Security Policies	28
Release 12.3X48-D10 Software Features	28
Application Layer Gateways (ALGs)	28
Chassis Cluster	28
Flow-Based and Packet-Based Processing	28
General Packet Radio Service (GPRS)	30
IP Tunneling	30

- IPv6 | 32
- Layer 2 Features | 32
- Network Address Translation (NAT) | 32
- PKI | 32
- Routing Protocols | 32
- Security | 34
- Unified Threat Management (UTM) | 34
- VPNs | 34

Changes in Behavior and Syntax | 36

Known Behavior | 37

- Authentication and Access Control | 37
- Chassis Clustering | 37
- Class of Service (CoS) | 37
- Flow-Based and Packet-Based Processing | 37
- Forwarding and Sampling | 38
- Network Management and Monitoring | 38
- Platform and Infrastructure | 39
- Unified Threat Management (UTM) | 39
- VPNs | 39

Known Issues | 40

- Flow-Based and Packet-Based Processing | 40
- Interfaces and Chassis | 41
- Platform and Infrastructure | 41
- Routing Policy and Firewall Filters | 42
- Routing Protocols | 42
- User Interface and Configuration | 42
- VPNs | 42

Resolved Issues | 43

- Resolved Issues: Release 12.3X48-D105 | 44
 - Flow-Based and Packet-Based Processing | 44
- Resolved Issues: Release 12.3X48-D100 | 44
 - Application Layer Gateways (ALGs) | 44
 - Chassis Clustering | 44
 - Flow-Based and Packet-Based Processing | 44

J-Web | 45

Network Management and Monitoring | 45

Routing Policy and Firewall Filters | 45

Resolved Issues: Release 12.3X48-D95 | 45

Flow-Based and Packet-Based Processing | 45

Network Management and Monitoring | 45

Platform and Infrastructure | 45

Routing Policy and Firewall Filters | 46

Resolved Issues: Release 12.3X48-D90 | 46

Application Layer Gateways (ALGs) | 46

Flow-Based and Packet-Based Processing | 46

Network Address Translation (NAT) | 47

Network Management and Monitoring | 47

Platform and Infrastructure | 47

Unified Threat Management (UTM) | 47

Switching | 47

Resolved Issues: Release 12.3X48-D85 | 47

Application Layer Gateways (ALGs) | 47

Flow-Based and Packet-Based Processing | 48

Intrusion Detection and Prevention (IDP) | 48

J-Web | 48

Network Management and Monitoring | 48

Platform and Infrastructure | 48

Routing Policy and Firewall Filters | 49

Routing Protocols | 49

Unified Threat Management (UTM) | 49

Resolved Issues: Release 12.3X48-D80 | 49

Application Layer Gateways (ALGs) | 49

Chassis Clustering | 49

Flow-Based and Packet-Based Processing | 49

Interfaces and Routing | 50

Intrusion Detection and Prevention (IDP) | 50

Network Address Translation (NAT) | 50

Platform and Infrastructure | 50

Routing Protocols	51
Services Applications	51
System Logs	51
Unified Threat Management (UTM)	51
VPNs	51
Resolved Issues: Release 12.3X48-D75	52
Flow-Based and Packet-Based Processing	52
Intrusion Detection and Prevention (IDP)	52
J-Web	52
Platform and Infrastructure	52
Routing Policy and Firewall Filters	53
Software Installation and Upgrade	53
Unified Threat Management (UTM)	53
VPNs	53
Resolved Issues: Release 12.3X48-D70	53
Application Layer Gateways (ALGs)	53
Authentication and Access Control	53
Chassis Cluster	53
Class of Service (CoS)	54
Flow-Based and Packet-Based Processing	54
Interfaces and Routing	54
J-Web	54
Layer 2 Ethernet Services	54
Network Address Translation (NAT)	54
Network Management and Monitoring	54
Platform and Infrastructure	55
Routing Protocols	55
Unified Threat Management (UTM)	55
VPNs	55
Resolved Issues: Release 12.3X48-D65	56
Application Layer Gateways (ALGs)	56
Flow-Based and Packet-Based Processing	56
Logical systems	56
Network Address Translation (NAT)	56

Network Management and Monitoring	56
Platform and Infrastructure	56
Switching	57
Resolved Issues: Release 12.3X48-D60 57	
Authentication and Access Control	57
Chassis Cluster	57
Flow-Based and Packet-Based Processing	57
J-Web	58
Logical Systems	58
Network Address Translation (NAT)	58
Network Management and Monitoring	58
Platform and Infrastructure	59
Routing Policy and Firewall Filters	59
User Interface and Configuration	59
VPNs	59
Resolved Issues: Release 12.3X48-D55 60	
Application Layer Gateways (ALGs)	60
Chassis Cluster	60
Flow-Based and Packet-Based Processing	61
Network Address Translation (NAT)	61
Network Management and Monitoring	61
Platform and Infrastructure	62
Routing Policy and Firewall Filters	62
VPNs	62
Unified Threat Management (UTM)	63
Resolved Issues: Release 12.3X48-D50 63	
Application Layer Gateways (ALGs)	63
Chassis Cluster	63
Ethernet Switching	64
Flow-Based and Packet-Based Processing	64
J-Web	64
Network Address Translation (NAT)	65
Network Management and Monitoring	65
Platform and Infrastructure	65

User Interface and Configuration	66
VPNs	66
Resolved Issues: Release 12.3X48-D45	66
Application Layer Gateways (ALGs)	66
Chassis Cluster	67
CLI	67
Ethernet Switching	67
Flow-Based and Packet-Based Processing	68
Forwarding and Sampling	69
Interfaces and Routing	69
J-Web	69
Network Address Translation (NAT)	70
Network Management and Monitoring	70
Platform and Infrastructure	70
Routing Policy and Firewall Filters	71
Routing Protocols	71
Unified Threat Management (UTM)	71
VPNs	71
Resolved Issues: Release 12.3X48-D40	72
Application Layer Gateways (ALGs)	72
Authentication and Access Control	72
Chassis Clustering	72
Flow-Based and Packet-Based Processing	72
Infrastructure	73
Interfaces and Routing	73
Intrusion Detection and Prevention (IDP)	73
J-Web	73
Network Address Translation (NAT)	74
Network Management and Monitoring	74
Platform and Infrastructure	74
Routing Policy and Firewall Filters	75
System Logs	75
Unified Threat Management (UTM)	75
VPNs	76

Resolved Issues: Release 12.3X48-D35 | 76

- Application Layer Gateways (ALGs) | 76**
- Chassis Cluster | 76**
- Flow-Based and Packet-Based Processing | 77**
- Network Address Translation (NAT) | 77**
- VPNs | 77**

Resolved Issues: Release 12.3X48-D30 | 77

- Application Layer Gateways (ALGs) | 77**
- Chassis Cluster | 78**
- Class of Service (CoS) | 78**
- CLI | 78**
- Flow-Based and Packet-Based Processing | 78**
- General Routing | 79**
- Intrusion Detection and Prevention (IDP) | 79**
- Interfaces and Chassis | 79**
- J-Web | 80**
- Network Address Translation (NAT) | 80**
- Platform and Infrastructure | 80**
- Routing Policy and Firewall Filters | 81**
- Services Applications | 81**
- Unified Threat Management (UTM) | 81**
- VLAN Infrastructure | 81**
- VPNs | 81**

Resolved Issues: Release 12.3X48-D25 | 82

- Application Layer Gateways (ALGs) | 82**
- Chassis Clustering | 82**
- Flow-Based and Packet-Based Processing | 83**
- Hardware | 83**
- Interfaces and Chassis | 83**
- Intrusion Detection and Prevention (IDP) | 84**
- Layer 2 Ethernet Services | 84**
- Network Address Translation (NAT) | 84**
- Platform and Infrastructure | 84**
- Routing Policy and Firewall Filters | 85**

Unified Threat Management (UTM) | 85

User Firewall | 85

VPNs | 86

Resolved Issues: Release 12.3X48-D20 | 86

Application Layer Gateways (ALGs) | 86

Authentication and Access Control | 87

Chassis Cluster | 87

Class of Service (CoS) | 88

Dynamic Host Configuration Protocol (DHCP) | 88

Flow-Based and Packet-Based Processing | 88

Infrastructure | 89

Interfaces and Chassis | 90

Intrusion Detection and Prevention (IDP) | 90

J-Web | 90

Network Address Translation (NAT) | 91

Network Management and Monitoring | 91

Platform and Infrastructure | 91

Routing Policy and Firewall Filters | 93

Routing Protocols | 94

Unified Threat Management (UTM) | 94

User Interface and Configuration | 94

VPNs | 94

Resolved Issues: Release 12.3X48-D15 | 96

Application Identification | 96

Application Layer Gateways (ALGs) | 96

Chassis Cluster | 96

CLI | 97

Dynamic Host Configuration Protocol (DHCP) | 97

Flow-Based and Packet-Based Processing | 97

General Packet Radio Service (GPRS) | 98

Interfaces and Routing | 98

Intrusion Detection and Prevention (IDP) | 99

J-Web | 99

Network Address Translation (NAT) | 99

- Security Policies | 99
- System Logging | 99
- Unified Threat Management (UTM) | 100
- VPNs | 100

Resolved Issues: Release 12.3X48-D10 | 100

- Application Layer Gateways (ALGs) | 100
- Chassis Cluster | 101
- CLI | 102
- Dynamic Host Configuration Protocol (DHCP) | 102
- Flow-Based and Packet-Based Processing | 102
- Hardware | 103
- Installation and Upgrade | 103
- Interfaces and Routing | 104
- J-Web | 104
- Layer 2 Transparent Mode | 104
- Network Address Translation (NAT) | 104
- Security | 105
- System Logging | 105
- Unified Threat Management (UTM) | 105
- VPNs | 105

Documentation Updates | 107

- IPsec VPN User Guide for Security Devices | 108
- Various Guides | 108
- System Logs | 108

Migration, Upgrade, and Downgrade Instructions | 110

- Installation and Upgrade | 110
- Migrating Group VPN Servers and Members | 111
 - Migration Scenarios and Considerations | 111
 - Migration Scenario 1 | 112
 - Migration Scenario 2 | 113
 - Migration Scenario 3 | 115

Upgrading an AppSecure Device | 115

- Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 116

Product Compatibility | **117**

Hardware Compatibility | **117**

Transceiver Compatibility for SRX Series Devices | **117**

Finding More Information | **118**

Documentation Feedback | **118**

Requesting Technical Support | **119**

Self-Help Online Tools and Resources | **119**

Opening a Case with JTAC | **120**

Revision History | **121**

Introduction

Junos OS runs on the following Juniper Networks[®] hardware: ACX Series, EX Series, M Series, MX Series, PTX Series, QFabric, QFX Series, SRX Series, and T Series.

These release notes accompany Junos OS Release 12.3X48-D105 for the SRX Series. They describe new and changed features, known behavior, and known and resolved problems in the hardware and software.

Note: On SRX5000 line of devices with SRX5K RE-13-20 (the first generation Routing Engine), a software upgrade to Junos OS Release 12.3X48-D80 and higher releases might fail the pre-check due to insufficient space available on the compact flash. As a workaround, downgrade to Junos OS Release 12.3X48-D10 first and then upgrade to the target release or fresh install the target release using the USB install-media. For more information, see [TSB17655](#)

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at <https://www.juniper.net/documentation/software/junos/>.

New and Changed Features

IN THIS SECTION

- [Release 12.3X48-D105 Software Features | 13](#)
- [Release 12.3X48-D100 Software Features | 13](#)
- [Release 12.3X48-D95 Software Features | 13](#)
- [Release 12.3X48-D90 Software Features | 13](#)
- [Release 12.3X48-D85 Software Features | 14](#)
- [Release 12.3X48-D80 Software Features | 14](#)
- [Release 12.3X48-D75 Software Features | 14](#)
- [Release 12.3X48-D70 Software Features | 14](#)
- [Release 12.3X48-D65 Software Features | 15](#)
- [Release 12.3X48-D60 Software Features | 16](#)
- [Release 12.3X48-D55 Software Features | 16](#)
- [Release 12.3X48-D45 Software Features | 18](#)
- [Release 12.3X48-D40 Software Features | 18](#)
- [Release 12.3X48-D35 Hardware Features | 19](#)
- [Release 12.3X48-D35 Software Features | 19](#)

- [Release 12.3X48-D30 Software Features | 20](#)
- [Release 12.3X48-D25 Software Features | 23](#)
- [Release 12.3X48-D20 Software Features | 25](#)
- [Release 12.3X48-D15 Software Features | 26](#)
- [Release 12.3X48-D10 Software Features | 28](#)

Learn about new features and enhancements to existing features in Junos OS Release 12.3X48 for the SRX Series.

Release 12.3X48-D105 Software Features

There are no new features in Junos OS Release 12.3X48-D105 for the SRX Series devices.

Release 12.3X48-D100 Software Features

There are no new features in Junos OS Release 12.3X48-D100 for the SRX Series devices.

Release 12.3X48-D95 Software Features

- **JDPI-Decoder engine version upgrade (SRX Series)**—Starting in Junos OS Release 12.3X48D95, the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) engine is packaged along with the application signature package version 999 that includes the protobundle version 1.380.0-64.005 and the JDPI-Decoder engine version 5.3.0-56. You can upgrade the application signature package when a new signature package version is available.

[See [show services application-identification status](#).]

Release 12.3X48-D90 Software Features

There are no new features in Junos OS Release 12.3X48-D90 for the SRX Series devices.

Release 12.3X48-D85 Software Features

There are no new features in Junos OS Release 12.3X48-D85 for the SRX Series devices.

Release 12.3X48-D80 Software Features

Application Security

- **JDPI-Decoder engine separation from Junos OS (SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, SRX650, SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, SRX5800, and vSRX)**—Starting in Junos OS Release 12.3X48-D80, the Juniper Networks Deep Packet Inspection-Decoder (JDPI-Decoder) engine is separated from Junos OS and allows you to download the JDPI-Decoder engine along with the protobundle. This implementation allows you to upgrade the JDPI-Decoder engine separately without upgrading Junos OS.

[See [show services application-identification status.](#)]

Release 12.3X48-D75 Software Features

There are no new features in Junos OS Release 12.3X48-D75 for the SRX Series devices.

Release 12.3X48-D70 Software Features

There are no new features in Junos OS Release 12.3X48-D70 for the SRX Series devices.

Release 12.3X48-D65 Software Features

Ethernet Switching

- **Connectivity fault management (CFM) and link fault management (LFM) support for SRX210, SRX220, SRX240, SRX550, and SRX650 devices**—Starting in Junos OS Release 12.3X48-D65, connectivity fault management (CFM) and link fault management (LFM) for the Operation, Administration, and Maintenance (OAM) are supported on very-high-bit-rate digital subscriber line (VDSL) and Point-to-Point Protocol over Ethernet (PPPoE) interfaces in addition to the Ethernet interfaces. CFM support includes fault monitoring, path discovery, and fault isolation functionalities. LFM support includes discovery and link monitoring, remote fault detection, and remote loopback functionalities.

[See [Understanding Ethernet OAM Connectivity Fault Management](#).]

Interfaces and Routing

- **ARP throttle and ARP detect [SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800]**—Starting in Junos OS Release 12.3X48-D65, an ARP throttling mechanism is introduced for SRX Series devices.

Excessive ARP processing results in high utilization of Routing Engine CPU resources, resulting in deprivation of CPU resources to other Routing Engine processes. To provide protection against excessive ARP processing, you can now configure ARP throttle and ARP detect using the following configuration statements:

- **edit forwarding-options next-hop arp-throttle *seconds***
- **edit forwarding-options next-hop arp-detect *milliseconds***



CAUTION: We recommend that only advanced Junos OS users attempt to configure the ARP throttle and ARP detect feature. Improper configuration might result in high utilization of Routing Engine CPU resources, which can adversely affect other processes.

[See [arp-throttle](#) and [arp-detect](#).]

Release 12.3X48-D60 Software Features

High Availability

- **Support for dedicated Bidirectional Forwarding Detection (BFD)**—Starting with Junos OS Release 12.3X48-D60, dedicated microkernel is supported on SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, and SRX650 to improve BFD performance. This is an enhancement to the distributed mode. Enabling dedicated microkernel completely offloads the BFD daemon to the Packet Forwarding Engine microkernel by dedicating one CPU core to this process. This significantly improves the BFD failure-detection performance. Because we are allocating one of the Packet Forwarding Engine's CPU cores to the BFD daemon as a result, the device throughput performance is reduced.

To enable dedicated BFD on the SRX240, SRX550, and SRX650 devices, use the **set chassis dedicated-ukern-cpu** command.

To enable real-time BFD on the SRX100, SRX110, SRX210, and SRX220 devices, use the **set chassis realtime-ukern-thread** command.

[See [Understanding BFD for Static Routes for Faster Network Failure Detection](#), [Understanding Distributed BFD](#), [dedicated-ukern-cpu \(BFD\)](#), and [realtime-ukern-thread \(BFD\)](#).]

Network Management and Monitoring

- **SNMP support for monitoring GRE keepalive status for all SRX Series devices**—Starting with Junos OS Release 12.3X48-D60, you can monitor GRE interface status using remote network management. In earlier releases, you had to use a CLI command to check GRE keepalive status. Now the SNMP MIB `jnxOamMibRoot` helps you to monitor GRE keepalive status using remote network management. When GRE keepalive status is changed, this SNMP MIB generates SNMP trap `jnxOamGreKeepAliveTrapVars` to send notifications.

[See [Enterprise-Specific SNMP MIBs Supported by Junos OS](#).]

Release 12.3X48-D55 Software Features

Flow-Based and Packet-Based Processing

- **TCP out-of-state packet drop logging (SRX Series)**—Starting in Junos OS Release 12.3X48-D55, SRX Series devices support logging of unsynchronized TCP out-of-state packets that are dropped by the flow

module.

Within any packet-switched network, when demand exceeds available capacity, the packets are queued up to hold the excess packets until the queue fills, and then the packets are dropped. When TCP operates across such a network, it takes any corrective actions to maintain error-free end-to-end communications.

This feature enables packet recovery by logging the out-of-sync packets for error-free communication, and avoids database servers going out of sync.

TCP packet drop logging occurs when:

- TCP packets that trigger session creation are not synchronized.
- TCP three-way handshake in flow fails.
- TCP sequence check in flow fails.
- TCP SYN packets are received in TCP FIN state.

The unsynchronized TCP out-of-state packet drop log is a packet-based log, not a session-based log.

NOTE: TCP packets that are dropped by TCP-proxy and IDP are not logged.

[See [TCP Out-of-State Packet Drop Logging Overview](#).]

Release 12.3X48-D45 Software Features

Unified Threat Management (UTM)

- **SNI support for Web filtering on SRX Series devices**—In Junos OS Release 12.3X48-D45, Junos OS supports Server Name Indication (SNI) for local, Websense-redirect, and Enhanced Web Filtering (EWF). SNI is an extension of SSL/TLS protocol to indicate what server name the client is contacting over an HTTPS connection. SNI inserts the actual hostname of the destination server in client's hello message in clear text format before the SSL handshake is complete. Web filtering uses the SNI information for further processing or modifying the query. In this implementation, the SNI includes only the server name, and not the full URL of the server.

[See [Web Filtering Overview](#).]

Release 12.3X48-D40 Software Features

Dynamic Host Configuration Protocol (DHCP)

- **Cascaded DHCPv6 prefix delegation on SRX Series devices**—Junos OS release 12.3X48-D40 supports the cascaded DHCPv6 prefix delegation feature that allows the customer premises equipment (CPE) to delegate sub-prefixes to sub-CPEs and assign IPv6 addresses to end hosts through stateless address auto configuration (SLAAC), stateless DHCPv6, or stateful DHCPv6. The LAN interface supports these three kinds of address assignment through independent configurations for DHCPv6, stateless SLAAC, and stateful DHCPv6.

Network Address Translation (NAT)

- **PAT port capacity increase, interim logging, and block recycling**—In Junos OS Release 12.3X48-D40, increased PAT port capacity is supported on SRX5400, SRX5600, and SRX5800 devices with next-generation Services Processing Cards (SPCs) using the CLI option **port-scaling-enlargement**, at the `[edit security nat source]` hierarchy level.

Interim logging and block recycling for port block allocation (PBA) are supported on all SRX Series devices using the CLI options **interim-logging-interval** and **last-block-recycle-timeout** at the `[edit security nat source pool name port block-allocation]` hierarchy levels.

Platform and Infrastructure

- **High-priority queue on SPC for SRX5400, SRX5600, and SRX5800 devices with IOC2 and IOC3 line cards**—For the SRX5K-MPC (IOC2), the SRX5K-MPC3-100G10G (IOC3), and the SRX5K-MPC3-40G10G (IOC3), a new configuration option is supported in Junos OS Release 12.3X48-D40 that enables packets with specific Diff Serv code point (DSCP) precedence, inet-precedence, IEEE 802.1Q, and DHCPv6 for IPv6 traffic bits to enter a high-priority queue on the SPC on high-end SRX Series devices.

Junos OS Release 12.3X48-D40 supports two types of priorities, high and low. Higher-priority queues take precedence over lower-priority queues for forwarding packets to achieve higher rate and lower latency, while ensuring that low-priority queues are not starved (locked out).

To designate packets for the high-priority or low priority queues, use the **spu-priority** configuration statement at the **[edit class-of-service forwarding-classes class]** hierarchy level. A value of high places packets into the high-priority queue, and a value of low places packets into the low-priority queue.

Release 12.3X48-D35 Hardware Features

Wireless WAN

- **CBA850 3G/4G/LTE wireless WAN bridge**—Starting with Junos Release 12.3X48-D35, SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, and SRX650 devices support the CBA850 G/4G/LTE wireless WAN bridge. The CBA850 can be deployed as a primary WAN or as a backup WAN to the primary wired network for the services gateways.

[See [CBA850 3G/4G/LTE Wireless WAN Bridge Overview](#).]

Release 12.3X48-D35 Software Features

Interfaces

- **G.993.5 Vectoring support for VDSL modules on SRX Series devices**—Starting with Junos OS Release 12.3X48-D35, firmware version v2.16.0 is available for SRX-MP-1VDSL-A to support VDSL vectoring. Vectoring on VDSL reduces crosstalk and increases network bandwidth.

[See [Upgrading the VDSL PIC Firmware](#).]

Unified Threat Management (UTM)

- **TCP proxy enhancement support on SRX5400, SRX5600, and SRX5800 devices**— Starting with Junos OS Release 12.3X48-D35, the UTM Sophos antivirus (SAV) single session throughput is increased for optimizing tcp-proxy forwarding.

Release 12.3X48-D30 Software Features

Authentication and Access Control

The list below in this section provides you an overview and details of the integrated ClearPass authentication and enforcement features:

Integrated ClearPass on SRX550, SRX650, SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800 devices—Integrated ClearPass authentication and enforcement enables SRX Series devices and Aruba ClearPass to collaborate in protecting your company's resources by enforcing security at the user identity level, not the IP address of a user's device. Not only can you configure security policies that apply to a user by username or group regardless of the device used, you can also configure a policy that specifies a group of users and a device type. Focusing security policies on user identity gives you exceptional control. Additionally, the SRX Series device provides ClearPass with threat and attack logs associated with users to inform your security enforcement at the ClearPass end. ClearPass can authenticate users across wired, wireless, and VPN infrastructures, and as the authentication source, post that information to the SRX Series device. [See [Understanding the SRX Series Integrated ClearPass Authentication and Enforcement Feature.](#)]

- **Individual user query on SRX550, SRX650, SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800 devices**—Junos OS Release 12.3X48-D30 supports the integrated ClearPass authentication and enforcement feature that includes the user query function. User query allows you to configure supported SRX Series devices to automatically query the Aruba ClearPass server for individual user authentication information when ClearPass does not post that information to it.

[See [Understanding the Integrated ClearPass Authentication and Enforcement User Query Function.](#)]

- **Threat detection and notification to ClearPass on SRX550, SRX650, SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800 devices**—Junos OS Release 12.3X48-D30 supports the integrated ClearPass authentication and enforcement feature that includes the threat detection and notification function. This function allows the SRX Series device to filter detected events specifically for threats and attacks and send logs about them to the ClearPass Policy Manager.

[See [Understanding How the Integrated ClearPass Feature Detects Threats and Attacks and Notifies the CPPM.](#)]

- **User and role enforcement on SRX550, SRX650, SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800 devices**—Junos OS Release 12.3X48-D30 supports the integrated ClearPass authentication and enforcement feature that includes the user role and enforcement function. For this feature, the SRX Series device relies on Aruba ClearPass as its authentication source. With the user authentication

information provided by ClearPass, you can configure security policies and allow the SRX Series device to enforce them based on user identity (source identity) rather than relying on the IP address of a user's device. You can also use group, or role, identities in security policies.

[See [Understanding Enforcement of ClearPass User and Group Authentication on the SRX Series Devices.](#)]

- **Web API and message dispatcher on SRX550, SRX650, SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800 devices**—Junos OS Release 12.3X48-D30 supports the integrated ClearPass authentication and enforcement feature, which includes the Web API function. This function allows Aruba ClearPass to initiate a connection with the SRX Series device to provide it with user authentication and identity information.

[See [Understanding How ClearPass Initiates a Session and Communicates User Authentication Information to the SRX Series Device Using the Web API.](#)]

Flow-Based and Packet-Based Processing

- **DHCPv6 enhancements to support RFC6177 for SRX Series devices**—Starting with Junos OS Release 12.3X48-D30, new CLI commands are introduced to configure preferred prefix length and sub-prefix length in clients. A delegating router (DHCPv6 server) is provided with IPv6 prefixes and a requesting router (DHCPv6 client) requests one or more prefixes from the delegating router. When the client receives a valid DHCPv6 block it must then delegate to all active interfaces using a sub-prefix delegation.
- **Support for logical interface policer on SRX Series devices**—Starting with Junos OS Release 12.1X48-D30, the logical interface policer, also called an aggregate policer, is supported on all SRX Series devices. The logical interface policer is a two-color or three-color policer that defines traffic rate limiting. You can apply a policer to input or output traffic for multiple protocol families on the same logical interface without needing to create multiple instances of the policer.

See:

- [Logical Interface \(Aggregate\) Policer Overview](#)
- [logical-interface-policer](#)
- [Two-Color Policer Configuration Overview](#)
- [Example: Configuring a Two-Color Logical Interface \(Aggregate\) Policer](#)

VPNs

- **Group VPN members on SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, and SRX650 devices supported with Group VPNv2 servers**—Junos OS Release 12.3X48-D30 allows Group VPN (also referred to as Group VPNv1) members to interoperate with Group VPNv2 servers. Group VPNv1 and Group VPNv2 members can coexist for the same group in the network.

[For more information, see [“Changes in Behavior and Syntax” on page 36](#), [“Known Behavior” on page 37](#), and [“Migration, Upgrade, and Downgrade Instructions” on page 110](#) sections in this release note. Also, see [Group VPN Overview](#) for Group VPN members and [Group VPNv2 Overview](#) for Group VPNv2 servers.]

- **IPsec VPN session affinity**—Starting with Junos OS Release 12.3X48-D30, the IOC2 on SRX5400, SRX5600, and SRX5800 devices supports IPsec session affinity for IPsec tunnel-based traffic.

With the IOC, the flow module creates sessions for IPsec tunnel-based traffic before encryption and after decryption on its tunnel-anchored SPU and installs the session cache for the sessions so that the IOC can redirect the packets to the same SPU to minimize packet forwarding overhead.

To enable session affinity on the IOC2, you need to first enable session cache and then enable session affinity. For the IOC1, you do not have to enable session cache for enabling session affinity.

To enable session cache, you need to run the **set chassis fpc <fpc-slot> np-cache** command.

To enable IPsec VPN session affinity, use the **set security flow load-distribution session-affinity ipsec** command.

NOTE: Once you enable or disable session cache on the IOC2, a system restart is required.

For configuring Express Path on an SRX5000 line device with Modular Port Concentrator (MPC), enable NP cache on the IOC using the **set chassis fpc fpc-number np-cache** command. Then configure the security policy to determine if the session is for Express Path.

The **set chassis fpc fpc-number services-offload** command is deprecated.

To disable Express Path on an SRX5000 line device with MPC, use the **delete chassis fpc fpc-number np-cache** command.

The **delete chassis fpc fpc-number services-offload** command is deprecated.

[For more information, see [Understanding VPN Session Affinity](#), [Enabling VPN Session Affinity, session-affinity](#), [Understanding Session Cache](#), and [Express Path Overview](#).]

Release 12.3X48-D25 Software Features

Application Layer Gateways (ALGs)

- **TCP support for SIP ALG on SRX Series devices**— Starting with Junos OS Release 12.3X48-D25, the SIP ALG supports TCP along with UDP. The TCP support reduces traffic to the server by eliminating the need to reregister or refresh the server frequently.

IP Monitoring

- **Increasing IP monitoring capacity for SRX5000 line devices for IOC2 and IOC3**—Starting with Junos OS Release 12.3X48-D25, IOC2 and IOC3 on SRX5000 line devices support IP monitoring on both the primary and secondary nodes.

The following IOC2 MICs support IP monitoring:

- MIC with 20x1GE SFP Interfaces (SRX-MIC-20GE-SFP)— 20 ports
- MIC with 10x10GE SFP+ Interfaces (SRX-MIC-10XG-SFPP)—10 ports
- MIC with 1x100GE CFP Interface (SRX-MIC-1X100G-CFP)—1 port
- MIC with 2x40GE QSFP+ Interfaces (SRX-MIC-2X40G-QSFP)—2 ports

The following IOC3s support IP monitoring:

- SRX5K-MPC3-100G10G (2x100GE and 4x10GE ports)
- SRX5K-MPC3-40G10G (6x40GE and 24x10GE ports)

IP monitoring checks the end-to-end connectivity of configured IP addresses and allows a redundancy group to automatically fail over when the monitored IP address is not reachable through the reth interface. Both the primary and secondary nodes in the chassis cluster monitor specific IP addresses to determine whether an upstream device in the network is reachable.

Network Address Translation (NAT)

- **IPv6-to-IPv6 Network Address Translation**—Starting in Junos OS Release 12.3X48-D25, stateless IPv6-to-IPv6 network prefix translation, which is compliant with RFC 6296, is provided. This feature enables address independence and provides a one-to-one relationship between IPv6 addresses in an internal network and IPv6 addresses in an external network. This type of translation can be used to secure proprietary information, for example, by a mobile service provider using customers' phone numbers as IPv6 local host identifiers.

- **Port-overloading**—Starting in Junos OS Release 12.3X48-D25, the total number of public IP addresses for source NAT pools configured with the port-overloading-factor increases from 16 to 128. This increase enables support for the maximum number of sessions provided by the SRX5000 line.

System Logging

- **Stream log based on category for SRX Series devices** —Starting with Junos OS Release 12.3X48-D25, when forwarding logs using stream mode, all the categories can be configured for sending specific category logs to different log servers. For stream mode log forwarding, the transport protocol used between Packet Forwarding Engine and the log server can be UDP, TCP, or TLS, and it is configurable. The transport protocol used between the Routing Engine and the log server can only be UDP.

[See [Understanding System Logging for Security Devices](#)]

Unified Threat Management (UTM)

- **Enhanced Web Filtering (EWF) supports HTTPS traffic for SRX240, SRX550, SRX650, SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800 devices**—Starting with Junos OS Release 12.3X48-D25, EWF supports HTTPS traffic by intercepting HTTPS traffic passing through the SRX Series device. The security channel from the SRX Series device is divided as one SSL channel between the client and the SRX Series device and another SSL channel between the SRX Series device and the HTTPS server. SSL forward proxy acts as the terminal for both channels and forwards the cleartext traffic to the UTM. UTM extracts the URL from the HTTP request message.
- **Sophos Antivirus over SSL forward proxy supports HTTPS traffic for SRX240, SRX550, SRX650, SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800 devices**—Starting with Junos OS Release 12.3X48-D25, UTM Sophos Antivirus over SSL forward proxy supports HTTPS traffic by intercepting HTTPS traffic passing through the SRX Series device. The security channel from the SRX Series device is divided as one SSL channel between the client and the SRX Series device and another SSL channel between the SRX Series device and the HTTPS server. SSL forward proxy acts as the terminal for both channels and forwards the cleartext traffic to UTM. UTM extracts the URL and the file checksum information from cleartext traffic. The Sophos Antivirus scanner determines whether to block or permit the requests.

Release 12.3X48-D20 Software Features

Interfaces

- **CLI enhancement for interfaces operational command for SRX Series devices**—Starting with Junos OS Release 12.3X48-D20, a new **show interfaces terse zone** command is introduced. This command displays the zone name for each interface.

Screens

- **Improved logging and trapping for SRX Series devices**—Starting with Junos OS Release 12.3X48-D20, the system log information for IP-based session limits is enhanced to include more information. Each session-limit screen log now contains five tuples of information. The hard core screen SNMP trap interval can now be configured in the range from 1 second to 3600 seconds. The default interval is 2 seconds.

Security Policies

- **Setting the TCP MSS value per security policy for SRX Series devices**—Beginning with Junos OS Release 12.3X48-D20, two new options enable you to set the maximum segment size for TCP sessions per policy. The two options for the **set security policies from-zone zone to-zone zone policy policy-name then permit tcp-options** statement are **initial-tcp-mss tcp-mss-value** and **reverse-tcp-mss tcp-mss-value**.

Previously, a packet's maximum segment size could only be set globally, for all TCP sessions, using the **set security flow tcp-mss** statement.

[See [initial-tcp-mss](#), [reverse-tcp-mss](#), and [show security policies](#).]

VPNs

- **AutoVPN spokes and Auto Discovery VPN (ADVPN) partners supported on all high-end SRX Series devices**—Starting in Junos OS Release 12.3X48-D20, all high-end SRX Series devices can be configured as AutoVPN spokes and ADVPN partners. In Junos OS Release 12.3X48-D10, only branch SRX Series devices were supported as ADVPN partners.

NOTE: BGP and OSPF dynamic routing protocols are supported with AutoVPN. Only OSPF is supported with ADVPN.

[See [Understanding Auto Discovery VPN](#).]

- **IKEv2 AES-GCM for branch SRX Series and SRX5400, SRX5600, and SRX5800 devices with SPC2 (SRX5K-SPC-4-15-320)**—Starting in Junos OS Release 12.3X48-D20, support is provided for Protocol Requirements for IP Modular Encryption (PRIME), an IPsec profile defined for public sector networks in the United Kingdom. PRIME uses AES-GCM rather than AES-CBC for IKEv2 negotiations. Both PRIME-128 and PRIME-256 cryptographic suites are supported.

The following options are available:

- The **encryption-algorithm** options **aes-128-gcm** and **aes-256-gcm** are available for proposals configured at the `[edit security ike proposal proposal-name]` hierarchy level.
- Predefined proposals **prime-128** and **prime-256** are available at the `[edit security ike policy policy-name proposal-set]` and `[edit security ipsec policy policy-name proposal-set]` hierarchy levels.

[See [encryption-algorithm \(Security IKE\)](#), [proposal-set \(Security IKE\)](#), [proposal-set \(Security IPsec\)](#), and [Understanding Suite B and PRIME Cryptographic Suites](#).]

Release 12.3X48-D15 Software Features

Application Layer Gateways (ALGs)

- **464XLAT ALG traffic support for SRX Series devices**—Starting with Junos OS Release 12.3X48-D15, XLAT ALG traffic is supported for the FTP, RTSP, and PPTP ALGs. The 464XLAT architecture is a combination of stateless translation on the customer-side translator (CLAT) and stateful translation on the provider-side translator (PLAT). The 464XLAT architecture is used to translate the packet information of a device using the combination of stateless (translates private IPv4 address to global IPv6 addresses, and vice versa) and stateful (translates IPv6 addresses to global IPv4 addresses, and vice versa) translation.

[See [Understanding 464XLAT ALG Functionality](#) and [Understanding 464XLAT ALG Traffic Support](#).]

- **Scaling BLF support for UDP-based SIP ALG for SRX Series devices**—Starting with Junos OS Release 12.3X48-D15, the SIP ALG supports 65,000-byte SIP messages on the UDP protocol. In the scaling Busy Lamp Field (BLF) application, if every instance is around 500 bytes, the SIP ALG supports 100 instances in one SIP UDP message.

BLF support for UDP-based SIP ALG includes the following features:

- The device can send and receive 65,000-byte SIP messages.
- The SIP ALG can parse the 65,000-byte SIP messages and open the pinhole, if required.
- The SIP ALG regenerates the new jumbo SIP message if NAT is configured and the payload is changed.

[See [Understanding Scaling Busy Lamp Field Support for the UDP-Based SIP ALG](#).]

Intrusion Detection Prevention (IDP)

- **New Pattern Matching Engine for SRX Series Devices**—Starting with Junos OS Release 12.3X48-D15, a new pattern matching engine is introduced for the SRX Series IDP feature. This scanning mechanism helps improve performance and policy loading.

NOTE: Currently, there are no changes to the existing DFA. The device continues to accept custom signatures in the existing DFA syntax.

When IDP performs any scheduled or automatic installation of a new signature update, a commit is being performed and you can view this commit using the "show system commit" command which is done "by root via other" as shown below:

```
user@srx3600> show system commit
```

```
0    2017-05-23 02:32:49 BST by root via other
```

```
1    2017-05-22 02:32:01 BST by root via other
```

```
2    2017-05-21 02:31:54 BST by root via other
```

[See [show security idp policy-commit-status](#).]

Security Policies

- **Increase in number of address objects per policy for SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800 devices**—Starting with Junos OS Release 12.3X48-D15, the maximum number of address objects per policy will increase from 1024 to 4096. The maximum number of policies per context for SRX3400 and SRX3600 devices will increase from 10,240 to 40,000, and for SRX5400, SRX5600, and SRX5800 devices, from 10240 to 80,000.

[See [Best Practices for Defining Policies on SRX Series Devices](#).]

Release 12.3X48-D10 Software Features

Application Layer Gateways (ALGs)

- **MS-RPC ALG and Sun RPC ALG map table scaling for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, the MS-RPC ALG and Sun RPC ALG dynamically allocate new mapping entries instead of using a default size (512 entries). They also offer a flexible time-based RPC mapping entry that removes the mapping entry (auto-clean) without affecting the associated active RPC sessions, including both control session and data session.

[See [Understanding Sun RPC ALGs](#) and [Understanding Microsoft RPC ALGs](#).]

Chassis Cluster

- **Dual active-backup IPsec VPN chassis clusters for SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices**—Starting with Junos OS Release 12.3X48-D10, VPN tunnels can terminate on either node of an active/active chassis cluster pair. Both nodes in the chassis cluster can actively pass traffic through VPN tunnels at the same time.

NOTE: Z-mode flows occur when traffic enters an interface on a chassis cluster node, passes through the fabric link, and exits through an interface on the other cluster node. They are not supported with dual active-backup IPsec VPN chassis clusters.

[See [Understanding Dual Active-Backup IPsec VPN Chassis Clusters](#).]

Flow-Based and Packet-Based Processing

- **Allowing embedded ICMP packets for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, security flow allows embedded ICMP packets to pass through your device even when there is no session match. By default, an embedded ICMP packet is dropped if it does not match any session. Use the **allow-embedded-icmp** statement at the **[edit security flow]** hierarchy level to enable this feature. Once enabled, all packets encapsulated in ICMP pass through and no policy affects this behavior. This feature is useful when you have asymmetric routing in your network and you want to use traceroute and other ICMP applications on your device.

[See [allow-embedded-icmp](#).]

- **Enhanced security flow session command for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, the following updates have been made to the **show security flow session** command:
 - A new option, **policy-id**, allows you to query the flow session table by policy ID.
 - New output flags have been added in the command output. The three available flags are **flag**, **natflag1**, and **natflag2**.

[See [show security flow session](#) and [show security flow session policy-id](#).]

- **Express Path (formerly known as services offloading) on the SRX5000 line MPC for SRX5400, SRX5600, and SRX5800 devices**—Starting with Junos OS Release 12.3X48-D10, the SRX5K-MPC supports Express Path. Express Path is a mechanism for processing fast-path packets in the Trio chipset instead of in the SPU. This method reduces the long packet-processing latency that arises when packets are forwarded from network processors to SPUs for processing and back to IOCs for transmission.

The following features are supported:

- Support inter- and intra-Packet Forwarding Engine Express Path for IPv4
- Per-wing statistics counter of bytes and packets sent out over the wing
- LAG interfaces
- NAT for IPv4
- Active and backup chassis cluster

NOTE: The services offloading feature is renamed to *Express Path* starting in Junos OS Release 12.3X48-D10. Currently, the documents still use the term *services offloading*.

[See [Express Path Overview](#).]

- **Improved session close log for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, the session closed log message has been expanded to include information about the device sending the TCP RST. The new log message **session closed TCP [client | server] RST** simplifies troubleshooting by indicating whether it was the client or the server that sent the TCP RST.

```
Jan 12 13:51:04 user@host RT_FLOW: RT_FLOW_SESSION_CLOSE: session closed TCP
SERVER RST: 30.0.0.2/54584->50.0.0.2/8081 None 30.0.0.2/54584->50.0.0.2/8081
None None None None 6 p1 green red 250003018 1(60) 1(40) 2 UNKNOWN UNKNOWN
N/A(N/A) ge-11/0/0.0 UNKNOWN
```

```
Jan 12 13:53:44 user@host RT_FLOW: RT_FLOW_SESSION_CLOSE: session closed TCP
CLIENT RST: 30.0.0.2/46488->50.0.0.2/23 junos-telnet 30.0.0.2/46488->50.0.0.2/23
None None None None 6 p1 green red 240003072 2(100) 1(60) 2 UNKNOWN UNKNOWN
N/A(N/A) ge-11/0/0.0 UNKNOWN
```

[See [System Log Explorers](#).]

General Packet Radio Service (GPRS)

- **GTP GSN table ager for high-end SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, one SRX Series device supports 100,000 GSN entries per SPU and 250,000 GSN entries per CP. Prior to this release, each entry was saved permanently. To prevent GSN entry exhaustion caused by frequent short-time roaming among countries, visiting GSNs are recorded when subscribers access the home GPRS core network from visiting countries. These entries are not deleted when the subscribers return home, but no further traffic is passed. The GTP GSN table ager causes the idling GSN entries to time out, preventing inactive GSNs from taking up too much space.

[See [show security gprs gtp gsn statistics](#).]

- **SCTP association scaling for high-end SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, the capacity of SCTP is enhanced from 5000 associations to 20,000 associations per SPU.

[See [Understanding Stream Control Transmission Protocol](#).]

IP Tunneling

- **IPv6 tunneling control for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, the IPv6 tunneling control feature introduces new screens for tunneled traffic based on user preferences. By default, all tunneling traffic is allowed by the screens unless the external IP encapsulation matches the block criteria of any existing screen. You must enable the screens to control, allow, or block the transit of tunneled traffic. The following new screens are introduced in this feature:

- GRE 4in4 Tunnel
- GRE 4in6 Tunnel
- GRE 6in4 Tunnel
- GRE 6in6 Tunnel
- Bad Inner Header Tunnel

- IPinIP 6to4relay Tunnel
- IPinIP 6in4 Tunnel
- IPinIP 6over4 Tunnel
- IPinIP 4in6 Tunnel
- IPinIP ISATAP Tunnel
- IPinIP DS-Lite Tunnel
- IPinIP 6in6 Tunnel
- IPinIP 4in4 Tunnel
- IPinUDP Teredo Tunnel

[See [Understanding Screen IPv6 Tunneling Control.](#)]

IPv6

- **Transparent mode for IPv6 support extended for SRX Series devices**—The Transparent mode for IPv6 was supported on all high-end SRX Series devices. Starting with Junos OS Release 12.3X48-D10, transparent mode for IPv6 is also supported on all branch SRX Series devices.

[See [Understanding IPv6 Flows in Transparent Mode](#).]

Layer 2 Features

- **Secure wire mode and mixed mode (Layer 2 and Layer 3) support for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, secure wire mode and mixed mode are supported and the interface type of these modes is the same without cross talk. You can configure both Layer 2 and Layer 3 interfaces simultaneously using separate security zones. There is no routing among IRB interfaces or between IRB interfaces and Layer 3 interfaces. Also, the user logical system is not supported for Layer 2 traffic. However, you can configure the Layer 2 interface using the root logical system.

As with mixed mode, in secure wire mode you can configure both Layer 3 and secure wire interfaces simultaneously. In fact, you can configure Layer 3, Layer 2, and secure wire interfaces simultaneously, without traffic cross talk between any two of the three configured interfaces.

[See [Understanding Mixed Mode \(Transparent and Route Mode\)](#).]

Network Address Translation (NAT)

- **NAT64 IPv6 prefix to IPv4 address persistent translation for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, this feature, which is targeted at IPv6 mobile networks, is used with the dual-translation mechanism, 464XLAT, to enable IPv4 services to work over IPv6-only networks. It augments the existing NAT64 mechanism, which enables IPv6 clients to contact IPv4 servers by translating IPv6 addresses to IPv4 addresses (and vice versa). However, the existing NAT64 mechanism does not ensure a sticky mapping relationship for one unique end user. By configuring the new **address-persistent** option with a specific IPv6 prefix length for NAT64 translations in an IPv4 source NAT pool, a sticky mapping relationship is ensured between one specific IPv6 prefix and one translated IPv4 address.

[See [Understanding NAT64 IPv6 Prefix to IPv4 Address-Persistent Translation](#).]

PKI

- **Digital certificate validation for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, the PKI daemon on SRX Series devices performs X509 certificate policy, path, key usage, and distinguished name validation, as specified in RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

[See [Understanding Digital Certificate Validation](#).]

Routing Protocols

- **Virtual Router Redundancy Protocol version 3 (VRRPv3) for branch SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, the Internet protocol VRRP provides one or more backup devices when a statically configured device is used on a LAN. The devices share a virtual IP address, with one device designated as the primary devices and the others as backups.

VRRP is the combination of both IPv4 and IPv6. The VRRPv3 feature supports IPv4 and IPv6 VRRP groups, including IPv6 traps. When you configure VRRP IPV6 groups, you must set the virtual-link-local address or link-local-address value explicitly. Otherwise, the address will be automatically generated.

To enable VRRPv3, set the **version-3** statement at the **[edit protocols vrrp]** hierarchy level.

NOTE: To avoid having multiple primary devices in the network, the VRRPv3 IPv4 devices switch to the backup state when they receive a VRRPv2 IPv4 advertisement packet. Additionally, to avoid having multiple primary devices in your IPv6 network that are caused by checksum differences, you need to disable VRRP for IPv6 on the backup devices before you perform the VRRPv2 to VRRPv3 upgrade.

NOTE: When you enable VRRPv3, ensure that the protocol is enabled on all the VRRP devices in the network. This is because VRRPv3 does not interoperate with previous versions of VRRP.

[See [Junos OS Support for VRRPv3](#).]

Security

- **Secure wire interface mode and forwarding for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, secure wire allows interfaces to be mapped one-to-one for ingress-to-egress forwarding. It differs from transparent and route modes in that there is no switching or routing lookup to forward traffic. Policies and upper-layer security features permit traffic to be forwarded through the device.

This feature is available on Ethernet logical interfaces; both IPv4 and IPv6 addresses are supported. You can configure interfaces for access or trunk mode. Secure wire supports chassis cluster redundant Ethernet interfaces and virtual LAN tagging, but it does not support IRB interfaces. This feature does not support security features not supported in transparent mode, including NAT and IPsec VPN. It does support Layer 7 features, including AppSecure, IPS, and UTM.

[See [Understanding Secure Wire.](#)]

Unified Threat Management (UTM)

- **Redirect Web filtering support for SRX Series devices**—The redirect Web filtering solution intercepts HTTP requests and sends them to an external URL filtering server, provided by Websense, to determine whether to block or permit the requests.

[See [Understanding Redirect Web Filtering.](#)]

VPNs

- **Auto Discovery VPN (ADVPN) protocol for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, AutoVPN deployments can use the ADVPN protocol to dynamically establish spoke-to-spoke VPN tunnels. When passing traffic from one spoke to another spoke, the hub can suggest that the spokes establish a direct security association, or "shortcut," between each other. Shortcuts can be established and torn down dynamically, resulting in better network resource utilization and reduced reliance on a centrally located hub.

On the hub, configure **advpn suggerter** at the **[edit security ike gateway gateway-name]** hierarchy level. On spokes, configure **advpn partner** at the **[edit security ike gateway gateway-name]** hierarchy level. ADVPN is supported with IKEv2 only.

[See [Understanding Auto Discovery VPN.](#)]

- **AutoVPN with traffic selectors for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, AutoVPN hubs can be configured with multiple traffic selectors. This allows hubs to advertise spoke networks with different metrics.

This feature includes the following added functionality:

- AutoVPN hubs with traffic selectors can be configured with the st0 interface in point-to-point mode for both IKEv1 and IKEv2.

NOTE: Dynamic routing protocols are not supported with traffic selectors with st0 interfaces in point-to-point mode.

- Traffic selectors are configured on the hub to protect traffic to spokes. Spokes can be non-SRX Series devices.

[See [Understanding AutoVPN with Traffic Selectors.](#)]

- **Enhanced VPN support for inactive-tunnel reporting and syslog for SRX Series devices**—Starting with Junos OS Release 12.3X48-D10, the methods used for debugging issues in VPN have been enhanced to improve the process in several ways. The use of CLI per-tunnel debugging, deleting the traceoptions configuration stanza after data collection is complete, and issuing the subsequent commit command are no longer required. Debugging can now be performed through Junos OS operational commands with the following VPN enhancements:

- Information shown in the output of the **show security ipsec inactive-tunnel** command
- System log messages

[See [Understanding Tunnel Events.](#)]

RELATED DOCUMENTATION

[Changes in Behavior and Syntax](#) | 36

[Known Behavior](#) | 37

[Known Issues](#) | 40

[Resolved Issues](#) | 43

[Documentation Updates](#) | 107

[Migration, Upgrade, and Downgrade Instructions](#) | 110

Changes in Behavior and Syntax

Junos OS Release 12.3X48-D105 does not have any changes in behavior and syntax.

RELATED DOCUMENTATION

New and Changed Features	 12
Known Behavior	 37
Known Issues	 40
Resolved Issues	 43
Documentation Updates	 107
Migration, Upgrade, and Downgrade Instructions	 110

Known Behavior

This section contains the known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 12.3X48.

Authentication and Access Control

- The maximum total group length in an LDAP response is 256 bytes. [PR1195365](#)

Chassis Clustering

- In rare situations, RG1+ failover due to the failure of an FPC or SPU might trigger MAC move protection on the neighboring switch. [PR1333505](#)
- IP monitoring for redundancy groups might not work on the secondary node if the reth interface has more than one physical interface configured. This is because the backup node sends traffic using the MAC address of the lowest port in the bundle. If the reply does not come back on the same physical port, then the internal switch drops the traffic. [PR1344173](#)

Class of Service (CoS)

- On SRX240 devices, some queues might not get enough packets when the traffic is high. [PR1061350](#)

Flow-Based and Packet-Based Processing

- Packets are dropped for the initial 15 seconds after the GRE tunnel is brought up over the VDSL interface. [PR821330](#)
- When you configure the TCP connections of the system log stream with a value greater than 1 (for example, a value of 3), the redundancy group's failover clears the log connections and re-creates the TCP log connections. The value of the TCP connections is decremented, and the value is reduced to 2. [PR1038113](#)

- On SRX5400, SRX5600, and SRX5800 devices, network processor offloading and UTM cannot coexist. Network processor offloading is disabled automatically if UTM is enabled. [PR1059527](#)
- On SRX5400, SRX5600, and SRX5800 devices, packets go out of order when the device merges the prefragmented IPv6 packets and then fragments the merged IPv6 packets. [PR1090550](#)
- On SRX Series devices, Z-mode RT logs are not supported on chassis clusters that are running in active/active mode. [PR1325609](#)
- In an SRX Series chassis cluster set up with dual control links, if the primary control link flaps continuously for an extended duration, then the cluster might go into an unstable state. This can happen even if the secondary control link is configured and stable. [PR1338773](#)
- The dynamic address feed name must be shorter than 32 bytes. [PR1353681](#)
- SRX220 and SRX240 devices show that a license is added successfully with a colon (:) in the output of the request system license add command, even if no license key is entered. [PR1388155](#)

Forwarding and Sampling

- On SRX Series devices running Junos OS Release 12.3, configuration file archival through transfer-on-commit does not work with the SFTP URL. [PR1372024](#)

Network Management and Monitoring

- On SRX Series devices, when a GRE tunnel is configured over a physical interface that has rpf-check configured, traffic destined for the IP address of the GRE tunnel is dropped because reverse path forwarding fails. As a workaround, configure the rpf-check mode loose on the underlying physical interface instead of the default rpf-check. [PR1288342](#)
- On SRX Series devices, when BGP route change happens on a large scale, the devices trigger a protective scheme on the entire system to avoid the generation of core files. As a result, packets passing through SRX Series devices are dropped for a short period of time. [PR1418179](#)

Platform and Infrastructure

- When interface monitoring is enabled, the PPPoE interface becomes inactive after the reth interface is disabled. [PR1060590](#)

Unified Threat Management (UTM)

- On SRX Series devices, wildcards behave differently starting from Junos OS Release 12.1X47. [PR1270382](#)

VPNs

- On SRX Series devices, if an IPsec VPN tunnel is established using IKEv2, due to a bad SPI, packets might be dropped during CHILD_SA rekey when the device is the responder for this rekey. As a workaround, to ensure that the SRX Series devices are always the initiator for CHILD_SA rekey, set the lifetime-seconds to a lower value than it is set on the remote peer. The lifetime can be set under [edit security ipsec proposal]. [PR1129903](#)

RELATED DOCUMENTATION

[New and Changed Features | 12](#)

[Changes in Behavior and Syntax | 36](#)

[Known Issues | 40](#)

[Resolved Issues | 43](#)

[Documentation Updates | 107](#)

[Migration, Upgrade, and Downgrade Instructions | 110](#)

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 12.3X48-D105.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

Flow-Based and Packet-Based Processing

- When you disable the services offloading feature, a warning message is displayed that the device is not rebooted. [PR748673](#)
- When an FI: Cell underflow or FI: Aliasing on allocates error occurs, the system logs the error messages but does not raise a CMERROR alarm. [PR1076299](#)
- On SRX Series devices, in an IPv6 VRRP scenario, when a host sends router solicitation messages to the VRRP virtual IPv6 address, the VRRP master replies with router advertisement messages with the physical MAC address instead of the virtual MAC address. The secondary VRRP device replies to the router advertisement messages with a physical MAC address. As a result, the host has two default gateways installed and sends traffic directly to two devices but not to the VRRP virtual IP address. This issue affects VRRP function and traffic. [PR1108366](#)
- On vSRX, SRX1500, SRX4K, ACX5K, EX4600, QFX5100, QFX5110, QFX5200, QFX10,000 line of devices and NFX Series, when the user uses console management port to authenticate, the credentials used during device authentication are written to a log file in clear text. Refer to <https://kb.juniper.net/JSA10969> for more information. [PR1290331](#)
- On SRX Series devices, in an SSL proxy scenario, if Transport Layer Security (TLS) packets contain an Application-Layer Protocol Negotiation (ALPN) extension (RFC 7301), the ALPN extension is removed by the SSL proxy, resulting in negotiation failure of the application-layer protocol (for example, HTTP/2). [PR1360820](#)
- When a commit is performed twice in succession, you might see a warning for the Enhanced Web Filtering (EWF) license if EWF is configured and a valid license is applied. [PR1362880](#)
- On SRX3000 line of devices with chassis cluster, when a node joins the chassis cluster, a very small amount of packet drop might occur on the active node during 100 msec. [PR1373545](#)
- VPN tunnels flap after a group is added or deleted in edit private mode on a clustered setup. [PR1390831](#)
- SRX Series devices cannot obtain a global IPv6 address through DHCPv6 when using a PPPoE interface with a logical unit number greater than 0. [PR1402066](#)

- The PKI keys exported using the command `run request security pki key-pair export` on Junos OS might have insecure file permissions. This might allow another user on the Junos OS device with shell access to read them. [PR1419515](#)
- On SRX5400, SRX5600, and SRX5800 devices with high availability (HA) in Z mode, a session might be in the backup state on both nodes (the expected working state is active/backup instead of backup/backup) if the corresponding route to the session is out of sync between nodes in a rare case. As a result, the fragmented traffic for the session gets looped on the fabric (fab) interface between the nodes. [PR1465100](#)

Interfaces and Chassis

- When more than 200 Virtual Router Redundancy Protocol (VRRP) groups are configured, the CPU of the Routing Engine becomes very busy, and the `show vrrp` command fails to run, leading to a timeout error message. As a workaround, increasing the advertisement interval of the VRRP protocol data unit (PDU) can reduce the pressure on the CPU of the Routing Engine. [PR1054359](#)

Platform and Infrastructure

- On SRX Series devices running FreeBSD 6-based Junos OS software, when a USB flash device with a mounted file system is physically detached by a user, the system might panic. The issue is resolved with FreeBSD 10 and later (Upgraded FreeBSD). [PR695780](#)
- When you use multicast with more than 600 copies of a multicast packet for a multicast group, the flowd process might crash while committing a change of multicast configuration. [PR986592](#)
- On SRX Series devices, mgd core files are generated during RPC communication between the SRX Series device and Junos Space or Junos OS CLI if the % symbol is present in the description or annotation. [PR1287239](#)
- Datapath debugging allows commits that have a missing configuration. [PR1295796](#)
- On the SRX5000 line of devices, the em-interface is an internal interface. If the em-interface goes down, the control link is lost, and the SRX Series cluster has an abnormal status. [PR1342362](#)
- The PICs might go offline and a split-brain scenario might be seen when interrupt storm happens on the internal Ethernet interface em0 or em1. [PR1429181](#)
- On the SRX5000 line of devices running Junos OS Release 12.3X48, in rare cases the request system software delete-backup command does not actually delete the old Junos OS package. As a workaround, you can manually delete the old Junos OS package at `/cf/packages/`. [PR1484228](#)

Routing Policy and Firewall Filters

- In a rare case, a specific domain is not resolved by the SRX Series devices when using the DNS address book. This is because the DNS library resolver fails to identify the pointer with a big offset in the compressed DNS name. [PR1471408](#)
- On SRX Series devices that have a security policy counter deployed, the count option in the security policy might not work. As a result, issuing show security policies <> detail might not print traffic statistics for the security policy. [PR1471621](#)

Routing Protocols

- In rare cases, when one node has been upgraded and failover is complete, the ppmdd process might lose connection to the new master. This can lead to the generation of a ppmdd core file. [PR1347277](#)
- On all platforms running Junos OS, an internal route leak might occur between routing instances. If when both instance import and instance export policies contain as-path-prepend actions. If this as-path is referred to some route, the rpd process might stop a change or delete an operation on the route (clearing BGP neighborhood, changing BGP or policy configuration, and so on). [PR1471968](#)

User Interface and Configuration

- On SRX Series devices, under certain conditions, if the configurations of the interface and security zone are not synchronized between the Routing Engine and the Packet Forwarding Engine, the interfaces might be bound to the NULL security zone. As a result, the network security (nsd) process might stop. [PR1000309](#)

VPNs

- In a dynamic VPN setup, when Pulse Secure clients are connected to the device, the clients are authenticated successfully and they receive IP address information from the device. However, the clients do not receive the secondary DNS information even though the secondary DNS information is configured on the device. [PR1016125](#)
- On SRX Series devices, when you change a data plane redundancy group number from one value to another (for example, from RG1 to RG4), traffic outage might occur. [PR1302846](#)

- On all SRX Series devices, if there is a period (.) in the configured CA profile name, the PKI daemon runs into issues after a device restart or a pki-service restart, causing PKI daemon related issues such as CRL download failure. [PR1351727](#)

RELATED DOCUMENTATION

New and Changed Features	 12
Changes in Behavior and Syntax	 36
Known Behavior	 37
Resolved Issues	 43
Documentation Updates	 107
Migration, Upgrade, and Downgrade Instructions	 110

Resolved Issues

This section lists the issues fixed in the Junos OS main release and the maintenance releases.

For the most complete and latest information about known Junos OS defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

Resolved Issues: Release 12.3X48-D105

Flow-Based and Packet-Based Processing

- Introduction of default inspection limits for application identification to optimize CPU usage and improve resistance to evasive applications. [PR1454180](#)

Resolved Issues: Release 12.3X48-D100

Application Layer Gateways (ALGs)

- The flowd or srpxfe process might stop when an ALG creates a gate with an incorrect protocol value. [PR1474942](#)

Chassis Clustering

- When the primary node is rebooted, it might take eight minutes for the traffic to pass through the secondary node. [PR1460207](#)

Flow-Based and Packet-Based Processing

- The flowd process stops and generates core files. [PR1438445](#)
- The SPC might hang on the SRX5000 line of devices. [PR1439744](#)
- If J-Flow version 9 is configured on SRX Series devices, the flowd process might stop. [PR1444803](#)

J-Web

- Getting error while changing the number of lines to display in J-Web. [PR1482050](#)

Network Management and Monitoring

- The flowd or srpxfe process might crash immediately after committing the J-Flow version 9 configuration or after upgrading to affected releases. [PR1471524](#)

Routing Policy and Firewall Filters

- The nstraced process might crash due to a memory allocation failure. [PR1445172](#)
- Traffic might be dropped when policies are changed in SRX Series devices. [PR1454907](#)
- The nsd process might get stuck and cause problems. [PR1458639](#)

Resolved Issues: Release 12.3X48-D95

Flow-Based and Packet-Based Processing

- The flowd process stops and all cards are brought offline. [PR1406210](#)
- Security logs cannot be sent to the external syslog server through TCP. [PR1438834](#)
- The IKE pass-through packet might be dropped after a NAT operation on the source. [PR1440605](#)
- The flowd process stops multiple times on SRX Series devices. [PR1453739](#)

Network Management and Monitoring

- Control links are logically down on SRX Series devices when the software version is Junos OS Release 12.3X48. [PR1458314](#)

Platform and Infrastructure

- The following log is generated every 5 seconds: **No Port is enabled for FPC# on node0.** [PR1335486](#)
- Upgrade limitations for Junos OS Release 12.3X48-D80, Junos OS Release 12.3X48-D85, and Junos OS Release 12.3X48-D90 on SRX5400, SRX5600, and SRX5800 devices with SRX5K RE-13-20 due to the following error: **The /cf filesystem is low on free disk space.** For more information, see [TSB17655](#) and [PR1458501](#).

Routing Policy and Firewall Filters

- The nsd process might stop due to a memory corruption issue. [PR1419983](#)
- The nsd process might get stuck and cause problems. [PR1458639](#)

Resolved Issues: Release 12.3X48-D90

Application Layer Gateways (ALGs)

- The TCP reset packet is dropped when any TCP proxy based feature and the **rst-invalidate-session** command are enabled simultaneously. [PR1430685](#)

Flow-Based and Packet-Based Processing

- Unable to access to SRX Series platforms if the messages **kern.maxfiles limit exceeded by uid 65,534, please see tuning(7)** are seen. [PR1402242](#)
- When a GRE tunnel (GRE-over-IPsec tunnel) or IPsec tunnel is used on an SRX Series device, the MTU of the tunnel interface is calculated incorrectly (24 bytes less than the expected value). [PR1426607](#)
- On SRX5400, SRX5600, SRX5800 platforms acting as a middle device between Internet Key Exchange (IKE) peers, it is not possible to establish more than one Encapsulating Security Payload (ESP) session between two IPv6 IKE peers if the IKE ALG is enabled on the middle SRX Series device. [PR1435687](#)

Network Address Translation (NAT)

- The nsd process stops and causes the Web filter to stop working. [PR1406248](#)

Network Management and Monitoring

- On SRX1400, SRX3400, and SRX3600 devices, the hardware error information collection might be abnormal with `test_WRED_committed_counter_error` messages. [PR1425447](#)

Platform and Infrastructure

- The CPU utilization might be very high and the forwarding plane might be stuck if J-Flow version 9 is configured. [PR1433961](#)

Unified Threat Management (UTM)

- SRX Series: srxpfe process crash occurs while JSF/UTM module parses specific HTTP packets (CVE-2019-0052). [PR1406403](#)

Switching

- Transit traffic might not work if the VLAN interface is used to loop back the packet from one interface to another. [PR1432728](#)

Resolved Issues: Release 12.3X48-D85

Application Layer Gateways (ALGs)

- The IPsec traffic might be blocked by SRX5000 line devices if they are acting as IPsec transit devices. [PR1372232](#)
- On all SRX Series platforms, SIP/FTP ALG does not work when SIP traffic with source NAT goes through the SRX Series devices. [PR1398377](#)

Flow-Based and Packet-Based Processing

- SSH to the loopback interface of the SRX Series device is not working properly when AppTrack is configured. [PR1343736](#)
- The IPsec VPN traffic might be dropped on pass-through authentication on the SRX Series device after an IKE rekey. [PR1353779](#)
- On SRX Series platforms, if services offloading (also known as Express Path) is enabled in chassis cluster active/active mode, the traffic would be dropped for services offloading sessions installed on Redundancy Group 2+ (RG2+). As originally designed, services offloading does not work with active/active mode. With the fix of this PR, when active/active mode and services offloading are both enabled, the sessions on RG2+ will no longer be qualified as services offloading sessions and work as normal sessions instead, so the traffic would not be dropped anymore. [PR1415761](#)
- GRE packets being are dropped before entering the IPsec tunnel after reboot or restart of the routing process. [PR1423768](#)

Intrusion Detection and Prevention (IDP)

- Unable to deploy IDP due to the IDP configuration cannot be committed. [PR1374079](#)

J-Web

- The httpd-gk process crashes, leading to dynamic VPN failures and high Routing Engine CPU utilization (upto 100 percent). [PR1414642](#)

Network Management and Monitoring

- On SRX3400 and SRX3600 platforms with NP-IOC cards, when chassis cluster with services offload is configured, when one reth interface is down, outgoing packets are dropped on the NP-IOC card. [PR1362631](#)

Platform and Infrastructure

- Some error messages could be seen when running the **show interface extensive** command from CLI or Junos Space. [PR1380439](#)
- Complete device outage might be seen when an SPU vmcore happens. [PR1417252](#)

Routing Policy and Firewall Filters

- Memory leak in nsd causes configuration change not taking effect after a commit. [PR1414319](#)
- One new alarm is created **NSD fails to restart because subcomponents fail**. [PR1422738](#)

Routing Protocols

- The rpd process stopped after a duplicate secondary route was deleted. [PR1113319](#)

Unified Threat Management (UTM)

- The device may not look up the blacklist first in a local Web filtering environment. [PR1417330](#)

Resolved Issues: Release 12.3X48-D80

Application Layer Gateways (ALGs)

- The status of SIP ALG is disabled and the original SIP active sessions are affected, when SIP active sessions are created with standard port 5060. [PR1373420](#)
- Sun RPC data traffic for previously established ALG sessions might be dropped because it matches the gate, which contains old interface information. [PR1387895](#)

Chassis Clustering

- On the SRX550M device, the SFP transceiver does not work after the chassis reboot. [PR1347874](#)
- The VPLS connection fails after a node reboot. [PR1350587](#)
- The device in chassis cluster mode might be unresponsive if IP monitoring is enabled. [PR1366958](#)
- The SNMP trap was sending incorrect information. [PR1378903](#)

Flow-Based and Packet-Based Processing

- On SRX Series devices, a watchdog issue happens if the Routing Engine fails to update the watchdog timer every 3 minutes. The watchdog reboots the device. [PR1256840](#)
- The flowd process generates a core file when the SIP ALG is enabled. [PR1352416](#)

- In an IPsec VPN scenario, when the SRX device is acting as a pass-through device with IKE and with ALG enabled, the IPsec VPN traffic might be dropped on the SRX device after an IKE rekey. [PR1353779](#)
- In chassis cluster mode with the IPsec tunnel configured, packet loss is observed when the clear-text packets are processed. [PR1373161](#)
- On the SRX550 device, the unicast packets are sent incorrectly to all ports of the VLAN. [PR1372020](#)
- On SRX Series devices, the PIM register message might be dropped. [PR1378295](#)
- On SRX Series devices, the pkid process might stop after RG0 failover. [PR1379348](#)
- The device does not send messages **frag needed** and **DF set** back to the source host during path MTU discovery. [PR1389428](#)
- On SRX4600, SRX5400, SRX5600, and SRX5800 devices, if CPU utilization is high the BGP packets might get dropped. [PR1398407](#)

Interfaces and Routing

- Incorrect ingress packet per second is observed on the MPLS enabled interface. [PR1328161](#)

Intrusion Detection and Prevention (IDP)

- On the secondary node, the IDP installation fails. [PR1336145](#)
- The update of the IDP database fails. [PR1367952](#)

Network Address Translation (NAT)

- The SRX Series device might send the **noSuchInstance** value to the SNMP server in response to source NAT pool utilization OIDs. [PR1357840](#)
- Source NAT sessions might fail to be created when **port-overloading** or **port-overloading-factor** is configured. [PR1370279](#)

Platform and Infrastructure

- After a RADIUS request is successfully sent by a device running Junos OS, if the network goes down suddenly, the response sent by the RADIUS server is not received within the timeout period. In this scenario, the RADIUS request is sent again with an invalid socket descriptor, which leads to the crashing of the auditd process (process provides an intermediary for sending audit records to the RADIUS and/or TACACS+ servers). [PR1173018](#)
- On SRX5400, SRX5600, and SRX5800 devices, the packet captured by datapath-debug on an IOC2 card might be truncated. [PR1300351](#)

- Frequency logs are displayed on the SRX5400, SRX5600, and SRX5800 devices when the IOC card has the same identifier as the SPC PIC card. [PR1357913](#)
- On SRX Series devices in a chassis cluster, the cold synchronization process might slow down when there are many Packet Forwarding Engines installed on the device. [PR1376172](#)
- Junos OS upgrade might fail with the **validate** option after the **/cf/var/sw** directory is erroneously deleted. [PR1384319](#)
- On SRX Series devices, the login class with allowed days and specific access start and end date might not work correctly. [PR1389633](#)
- On SRX Series devices, the flowd process stops if it goes into a dead loop. [PR1403276](#)

Routing Protocols

- On SRX Series devices, dedicated BFD does not work. [PR1347662](#)

Services Applications

- If J-Flow version 9 is configured on the device, the flowd process might stop, causing traffic loss. [PR1370389](#)

System Logs

- The following log messages are displayed on the device: **L2ALM Trying peer/master connection, status 26**. [PR1317011](#)

Unified Threat Management (UTM)

- Some traffic from the webcam that contains non standard HTTP boundary format will cause the SRX Series devices UTM/SAV to hold traffic/mbuf and later causes failover. [PR1283806](#)

VPNs

- VPN tunnels might not be configured successfully, and the VPN tunnels might not come up. [PR1376134](#)
- Adding or deleting site-to-site manual NHTB VPN tunnels to an existing st0 unit causes the existing manual NHTB VPN tunnels under the same st0 unit to flap. [PR1382694](#)

Resolved Issues: Release 12.3X48-D75

Flow-Based and Packet-Based Processing

- Memory leak occurs due to TCP proxy. [PR1166058](#)
- The flowd process might stop when the **syn-proxy** function is used. [PR1343920](#)
- Policy and zone configuration are out of synchronization with the Packet Forwarding Engine. [PR1345397](#)
- On SRX650 and SRX3600 devices running Junos OS Release 12.3X48-D30, the **SECINTEL_FEED_DB_SAVE_FAILED** error message appears. [PR1350523](#)
- After a flowd process stops, the device reboots unexpectedly. [PR1353058](#)
- IPv6 backup sessions might be stuck and cannot be cleared after the data plane RGs failover. [PR1354448](#)
- PIM register messages stops unexpectedly from the source FHR. .
- On the secondary central point, the multicast session leaks for the PIM register occurs on the device. [PR1360373](#)

Intrusion Detection and Prevention (IDP)

- IDP signature update fails on the secondary node. [PR1358489](#)

J-Web

- The severity information is not displayed on the device for the event messages. [PR1335218](#)

Platform and Infrastructure

- The cscript core file is generated during pressure test. [PR843062](#)
- The VPN flaps during commits for the apply-groups. [PR1242757](#)
- In RSI, the mandatory arguments are missing for the **request pfe execute** and **show usp policy counters** commands. [PR1341042](#)
- Upon deletion of the reth interfaces from the configuration, the commit does not consider the IKE logical gateway interface (reth) configuration dependency. [PR1352559](#)

Routing Policy and Firewall Filters

- On SRX Series devices, the NSD process might stop on the Packet Forwarding Engine with large-scale security policy configuration. [PR1354576](#)

Software Installation and Upgrade

- The **request system reboot node in/at** command results in immediate reboot instead of rebooting at the allotted time. [PR1303686](#)

Unified Threat Management (UTM)

- On SRX devices configured with a UTM blacklist, legitimate websites might be blocked if they share the same IP with one URI that is in the list. [PR1180834](#)

VPNs

- All IPsec tunnels are in active and inactive state. [PR1348767](#)

Resolved Issues: Release 12.3X48-D70

Application Layer Gateways (ALGs)

- H323 ALG decode Q931 packet error is observed even after H323 ALG is disabled. [PR1305598](#)
- SIP calls drop due to 10,000 limit per SPU. [PR1337549](#)

Authentication and Access Control

- The uacd process is unstable after upgrading to Junos OS Release 12.3X48 and later. [PR1336356](#)

Chassis Cluster

- IP monitoring is working incorrectly when one node is in secondary-hold and the primary nodes priority is 0. [PR1330821](#)
- After the primary node or the secondary node is restarted, the FPC module goes offline at the secondary node. [PR1340116](#)

- The redundant power supply LED in the front panel LED turns off when the cluster configuration is modified. [PR1342886](#)

Class of Service (CoS)

- Packets go out-of-order on SRX5K-SPC-4-15-320 (SPC2) cards with IOC1 or FIOC cards. [PR1339551](#)

Flow-Based and Packet-Based Processing

- The embedded ICMP packets might be dropped when performing NAT64. [PR1328512](#)

Interfaces and Routing

- If the PPP interface is configured then traffic received on this interface is sometimes reordered. [PR1340417](#)

J-Web

- When you login to the web authentication page, the **BAD_PAGE_FAULT** error message is displayed. [PR1180787](#)
- Unable to delete dynamic VPN user configuration. [PR1348705](#)

Layer 2 Ethernet Services

- The **show vlans detail no-forwarding** command in RSI does not display any information since **no-forwarding** option is not supported. [PR1336267](#)

Network Address Translation (NAT)

- Arena utilization on an FPC might increase and then resume to a normal value. [PR1336228](#)

Network Management and Monitoring

- When the **source-address** option is configured on the syslog, the device might stop sending syslog messages after a reboot. [PR1333000](#)
- When configuring VRRP on a tagged interface, VRRP virtual IP address is not reachable. [PR1336290](#)

Platform and Infrastructure

- When you configure the http-get RPM probes, the URL might be lost in the get message. [PR1256865](#)
- IPsec VPN tunnels might go down when you commit the configuration from Junos Space, Junos script, or the J-Web. [PR1317664](#)
- The data plane does failover from node 0 to node 1 when one SPC stops unexpectedly. [PR1331809](#)
- After an upgrade, the ppmd process might stop under certain conditions. [PR1335526](#)

Routing Protocols

- OpenSSL security advisory [07 Dec 2017]; Refer to <https://kb.juniper.net/JSA10851> for more information. [PR1328891](#)

Unified Threat Management (UTM)

- For a security policy with HTTP pass-through firewall authentication being configured, it is recommended to configure web-redirect for HTTP pass-through firewall authentication instead of using direct HTTP pass-through firewall authentication because the web browser might automatically carry credentials in subsequent request to the target web-server. [PR1351457](#)

VPNs

- When the VPN tunnel is configured with traffic-selector and the traffic-selector is narrowed during negotiation (because of flex match), route added to narrow the traffic-selector remote subnet is not cleaned up when the corresponding VPN tunnel is removed. [PR1287171](#)
- IPsec traffic statistics counters return 32-bit values which might quickly overflow. [PR1301688](#)
- If an IP address on a tunnel interface is same as the external interface, the IPsec VPN might stop working after changing the tunnel IP address. [PR1330324](#)
- Unable to add commit check or commit validation due to design constraints. [PR1344125](#)

Resolved Issues: Release 12.3X48-D65

Application Layer Gateways (ALGs)

- Unexpected SIP ALG behavior might occur after upgrading to Junos OS Release 12.3X48. [PR1328266](#)

Flow-Based and Packet-Based Processing

- Datapath-debug does not capture traffic when only the np-ingress filter is applied. [PR1291194](#)
- The **fin-invalidate-session** command does not work when the Express Path feature is enabled on the SRX Series device. [PR1316833](#)
- Return traffic through routing instance might drop intermittently after changing the zone and routing instance configuration for the st0.x interface. [PR1316839](#)
- Flowd core files are generated on both nodes causing a traffic outage. [PR1324476](#)

Logical systems

- The OSPF peers are unable to establish neighbors between the LT interfaces of the logical systems. [PR1319859](#)

Network Address Translation (NAT)

- The proxy ARP does not work intermittently after RGO failover. [PR1289614](#)

Network Management and Monitoring

- The MIB OID ifHCOutOctets might rise to a huge number for 100 Mbps or 1 Gbps interfaces randomly. [PR1272233](#)
- Hardware-timestamp configuration in RPM probes shows unrealistic timestamps. [PR1313275](#)

Platform and Infrastructure

- A LU (or XL) and XM chip-based line card might go into a wedge condition. [PR1160079](#)
- The flowd process might stop if flow monitoring version 9 is used. [PR1306780](#)
- Firewall filter does not work as expected. [PR1316962](#)
- Memory leak is triggered by a communication issue between the Routing Engine and the Packet Forwarding Engine. [PR1321314](#)

Switching

- Double VLAN tagging (vlan-tags) not configurable after upgrade to Junos OS Release 12.3X48. [PR1310410](#)

Resolved Issues: Release 12.3X48-D60

Authentication and Access Control

- On SRX Series devices, when you use Integrated User Firewall (IUF), the user ID process might consume high CPU space. The traceoptions of IUF might have many **UGCALC_AD_MEMBER_UPDATE** messages. [PR1280783](#)

Chassis Cluster

- On all SRX Series devices in chassis cluster, when **lo0** interface is used as an external interface for an IPsec VPN tunnel, and the outgoing interfaces are local interfaces (non-reth interface), shutting down or rebooting the active node (the node processes the VPN traffic) causes the outgoing interface information of the ESP session missing, resulting in VPN traffic failure. [PR1202992](#)
- On SRX5600 and SRX5800 devices in a chassis cluster with dual control links configured, if you upgrade the devices to Junos OS Release 12.3X48-D55, the device results in having all the FPC cards offline post bootup at the upgraded nodes and will not be able to handle traffic. This issue does not affect Junos OS Release 12.3X48-D50 and earlier releases, and Junos OS Release 12.3X48-D60 and later releases are not affected. [PR1319208](#)

Flow-Based and Packet-Based Processing

- On all SRX Series devices, if the same flow session traverses the same device multiple times and this flow session requires TCP proxy on the device, then RG1+ failover might cause high rate of TCP probe packets between the TCP proxies, resulting in high SPU CPU utilization. [PR1268740](#)
- On all SRX Series devices, after performing an RG0 failover, if the traffic relies on the use of proxy-arps, the device might work incorrectly causing traffic outage. [PR1289614](#)
- When datapath-debug is enabled with np-ingress filter, the packets will not be captured. [PR1291194](#)
- On all SRX Series devices, if the device works as a DNS proxy that takes hostname resolution requests on behalf of the clients behind it, the name process might stop causing the hostname resolution to fail for the client. [PR1307435](#)
- On SRX3400 and SRX3600 devices, if there is a major communication issue between the Routing Engine and the Packet Forwarding Engine (running on the SPC card in SRX3400 and SRX3600 devices in chassis

cluster), the Routing Engine memory might leak due to high percentage of packet loss between the Routing Engine and Packet Forwarding Engine. [PR1321314](#)

J-Web

- On SRX Series devices, when you use J-Web to commit changes, the backslash character on the source identity object is removed. [PR1304608](#)
- On SRX Series devices, when you login using J-Web, the J-Web page displays memory exhaustion fatal error **Cannot log at JWEB - Fatal error: Allowed memory size of 20971520 bytes exhausted.** [PR1304926](#)
- On J-Web, fatal error message is seen in **Maintain->Software.** [PR1308638](#)
- The VPN configuration wizard fails to start. [PR1308663](#)
- J-Web authentication fails if the password includes the backslash character. [PR1316915](#)

Logical Systems

- If a logical system is configured with security policies, replacing the name of the logical system might cause the NSD process to stop. [PR1307876](#)

Network Address Translation (NAT)

- On SRX Series devices, the periodic execution of the **show security zones detail** command causes the NSD process to fail releasing of the unused memory and causes memory leak. [PR1269525](#)
- On SRX Series devices, embedded ICMP might cause the flowd process to stop (CVE-2017-10610). Refer to <https://kb.juniper.net/JSA10813> for more information. [PR1270680](#)

Network Management and Monitoring

- On SRX Series devices, when J-Flow is enabled for multicast traffic **extern nexthop** is installed during the multicast composite next hop. However, when you uninstall the composite next hop, it does not free the **extern nexthop**, which results in the J-tree memory leak. [PR1276133](#)
- The **show arp no-resolve interface X** command for nonexistent interface X is showing all unrelated static ARP entries. [PR1299619](#)

Platform and Infrastructure

- Automatic recovery of **Scheduler tick table parity error** for MPC3E/MPC4E/MPC5E/MPC6E/T4000-FPC5. [PR1083959](#)
- On SRX Series devices with chassis cluster, memory leak occurs when em0 or em1 interface is down. [PR1277136](#)
- On SRX5400, SRX5600, and SRX5800 devices, under a heavy flood of IPv6 neighbor discovery protocol (NDP) packets, some incoming IPv6 neighbor advertisements (NA) may be dropped due to a queue being full. This issue has been resolved by using a different queue for IPv6 NA packets. [PR1293673](#)
- Autoinstallation DHCP does not work after upgrading from Junos OS Release 12.1X44 to Junos OS Release 12.1X46. [PR1296178](#)
- On SRX100, SRX110, SRX210, and SRX220 devices, interface stops receiving multicast traffic after running **monitor traffic interface xxx** command. [PR1301212](#)

Routing Policy and Firewall Filters

- On SRX Series devices, during route flapping, high rpd CPU utilization is seen and stays high (above 90%) until the rpd is restarted. [PR953712](#)
- User firewall users are not assigned their roles. [PR1282744](#)
- The DNS configured in the address-book fails to resolve the IP address. [PR1304706](#)
- On SRX5400, SRX5600, and SRX5800 devices, if a logical system is configured containing security policies, replacing the name of a logical system might cause nsd process to stop. [PR1307876](#)

User Interface and Configuration

- Deactivated security policy was unexpectedly moved after new policy when **commit** was performed. [PR1248882](#)

VPNs

- The kmd process might stop in NAT-T scenario. [PR1302814](#)
- On SRX Series devices, with VPN and NAT-T enabled, core files might be generated. [PR1308072](#)
- On SRX5400, SRX5600, and SRX5800 devices, the match of the traffic selector might fail with the destination NAT, IPsec VPN session affinity, and multiple traffic selectors, blocking the traffic through IPsec VPN even if the VPN tunnel is established. [PR1309565](#)

Resolved Issues: Release 12.3X48-D55

Application Layer Gateways (ALGs)

- On SRX5400, SRX5600, and SRX5800 devices, the buffer for advanced security services (ALGs, UTM, and AppSecure) might be exhausted by heavy application traffic. For example heavy DNS traffic processed by DNS ALG causes buffer exhaustion, which impacts all the advanced security services, and causes the related application traffic outage. [PR1177189](#)
- On SRX Series device, the logs **RT_FLOW: FLOW_REASSEMBLE_SUCCEED:** packet merged are removed from syslog messages. If lots of fragmented packets are processed, and the force-ip-reassembly option is enabled or fragments merge is required by some Advanced Services (such as UTM, AppSecure, IDP, ALGs, GTP, SCTP, and etc.), if the logs from syslog **RT_FLOW: FLOW_REASSEMBLE_SUCCEED:** Packet merged are seen then this might cause high CPU usage on Routing Engine (RE). [PR1278333](#)

Chassis Cluster

- On SRX100, SRX110, SRX220, and SRX240 Series devices, the console connection shows corrupt outputs when **set system ports console silent-with-modem** is configured. [PR1245386](#)
- SRX Series devices, an interface is not synced between the Routing Engine (RE) and the Packet Forwarding Engine under HA cluster environment when some special Class of Service (CoS) setting is configured. [PR1248193](#)
- On SRX-Series devices with chassis cluster configured, there is no **commit error or warning** message when you **commit** check phase with the use of interface monitoring or IP-monitoring for High Availability (HA) under Redundancy Group 0 (RG0). It is not recommended to configure chassis cluster interface monitoring on RG0 for devices. Without a **commit error or warning**, it might be end up with a non-recommended or unsupported configuration for HA failover that can cause a production impact. [PR1261420](#)
- On SRX Series devices, the Virtual Router Redundancy Protocol (VRRP) advertisements might not be sent out when packets passes through the switching fabric (SWFAB) link on chassis cluster. [PR1272576](#)
- On SRX Series devices in a chassis cluster, the FTP data session might hang after two back to back RG1+ failovers. [PR1286547](#)
- On SRX Series devices, during configuration changes on the device through NETCONF or Junos Space, the device returns a **warning** message with a wrong error tag that prevents the configuration from being committed and the device fails to get added to the Junos Space. [PR1286903](#)

Flow-Based and Packet-Based Processing

- On SRX Series devices in a chassis clusters, if local interfaces (non-reth interface) are used, the IPv4 sessions flowing on the local interfaces might go into backup state on both nodes, which causes stale sessions to be created. [PR1247288](#)
- On SRX5400, SRX5600, and SRX5800 Series devices, when the Services Processing Unit (SPU) stops working, the core file might get created empty. [PR1249547](#)
- On SRX Series devices, a core file is generated when traffic causes high memory usage and lot of memory allocation failures are observed at Deep Packet Inspection (DPI) module. The core file is difficult to reproduce and high memory usage might not always result in core file. The core file is generated due to buffering issues in DPI engine code when the application identification requires data to be buffered at engine. [PR1266517](#)
- On SRX5400, SRX5600, and SRX5800 Series devices, when the NAT is configured, the traceroute traffic might drop. [PR1266611](#)
- On SRX Series devices, non-IPv4 packets are dropped if double GRE IPv4 encapsulation is used. [PR1270070](#)
- On SRX Series devices, when the Dynamic Host Configuration Protocol (DHCP) or DHCP relay is configured, specially crafted packet might cause the flowd process to stop, halting or interrupting traffic from flowing through the devices. [PR1270493](#)
- On SRX Series devices, a core file might be generated if the mirror-filter port is down. [PR1270724](#)
- On SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800 devices, if Data Path Debugging is enabled, the flow session might hang after inactivity for five minutes. [PR1291749](#)

Network Address Translation (NAT)

- On SRX Series devices, when NAT is configured, the nsd process might get a memory leak after a NAT configuration change and commit. [PR1260409](#)

Network Management and Monitoring

- On SRX Series devices, the syslog messages from the secondary node might not reach the syslog server when reth interface is source interface for syslog. This issue does not impact traffic. [PR1252128](#)
- On SRX Series device, when you do a SNMP walk for operating temperature using **show snmp mib walk jnx Operating Temp**, the temperature reading of PEMs and CB are not seen. [PR1263534](#)
- On SRX1400, SRX3400, and SRX3600 devices with a NP-IOC card installed, the data-plane related to the NP-IOC card might hang causing the child interfaces to be removed from the ae/reth LAG when the LACP is enabled. [PR1285011](#)

Platform and Infrastructure

- On SRX Series devices, additional **UI_CFG_AUDIT** messages are logged for private configuration session and does not have adverse effect to the operational state of the device. [PR1261147](#)
- On SRX5400, SRX5600, and SRX5800 Series devices in a chassis cluster, if sampling is used, the flowd process fails and core files are seen on both the nodes, when route is updated through dynamic protocols, such as BGP. [PR1249254](#)
- On SRX Series devices, the routes activated by IP-Monitoring are not getting cleared after the probe status changes from Fail to Pass. The **show services ip-monitoring status** shows the route **NOT-APPLIED** but **show route** might show ip-monitoring route active (Static route with preference 1). [PR1263078](#)
- On SRX5400, SRX5600, and SRX5800 devices with chassis cluster Z-mode scenario, the Time To Live (TTL) of some Z-mode packets is reduced to zero by mistake if IOC2 or IOC3 interface is configured as HA fabric port, and some Z-mode packets with a size greater than 212 bytes might be sent to SPC1 causing the traffic to be dropped. [PR1270770](#)
- On SRX Series devices, the secondary node in a chassis cluster environment might stop or go into DB mode, displaying the **panic:rn timer_index_alloc** message. This issue is sometimes observed in a chassis cluster environment with multipoint st0.x interface configured, and the tunnel interfaces flaps according to IPsec idle-timeout or IPsec VPN-monitor. [PR1244491](#)
- On SRX Series devices, the **abnormal timer recovery** error message is displayed frequently in the logs, without any service impact. [PR1260274](#)

Routing Policy and Firewall Filters

- On SRX Series devices, when a single event upset (SEU) occurs on a scheduler's SRAM and on an XM chip (SCHED), you need to perform power-reset (off-line and on-line/cold boot) an affected FPC to recover. With this fix, the correction is done by the software and not necessary to perform power-reset. [PR1083959](#)
- On SRX Series devices, the DNS resolutions sent out through a custom routing instance do not work, if there is no route to the DNS server existing in default routing instance. [PR1287893](#)

VPNs

- On SRX5400, SRX5600, and SRX5800 devices, the st0 interface global counter statistics does not increment and remains zero, although traffic passes through the tunnel sub-interfaces such as st0.0 and st0.1. [PR1171958](#)
- On SRX Series devices, traffic is lost after adding traffic selector in a IPsec VPN. [PR1249908](#)
- On SRX Series devices, when st0 interface is moved from one routing instance to another routing instance, packet loss is observed. [PR1255593](#)

- On SRX Series devices with Chassis Cluster, the **ksyncd** might stop and the next hop of point to multi-point (P2MP) tunnel does not work correctly on secondary node if routing-instances with graceful-restart is running. [PR1260270](#)
- On SRX Series devices, manual Next Hop Tunnel Binding (NHTB) does not work on Junos OS 15.1X and 12.3X releases. The following error is displayed on the IKE traces **Internal Error: Manual NHTB add failed**. [PR1266797](#)
- On SRX Series devices, if traffic-selector is configured, the IKE redundant gateway failover fails. [PR1270000](#)
- On SRX Series devices, when a local certificate is used for the IPsec VPN, CA revokes the IPsec VPN and CRL checking is enabled. The pkid process might stop. [PR1290218](#)

Unified Threat Management (UTM)

- On SRX Series devices, when http-reassemble is configured, the UTM Web filter might block the non-http traffic over port 80 (for example, RTMP traffic over port 80). [PR1267317](#)
- On SRX Series devices, when you use UTM (includes Anti-Spam, Content-Filtering, and Anti-Virus) scanning on e-mail protocol traffic, the e-mail flow might stop at some point and UTM traceoptions indicates **MIME deadlock detected**. [PR1265992](#)

Resolved Issues: Release 12.3X48-D50

Application Layer Gateways (ALGs)

- On SRX5400, SRX5600, and SRX5800 devices, the buffer for advanced security services (ALGs, UTM, and AppSecure) might be exhausted by heavy application traffic. For example heavy DNS traffic processed by DNS ALG causes buffer exhaustion, which impacts all the advanced security services, and causes the related application traffic outage. [PR1177189](#)
- On SRX Series devices with ISC BIND software, upgraded to resolve multiple vulnerabilities. These issues only affect devices where the DNS proxy service is enabled. The DNS proxy feature is disabled by default. Refer to JSA10785 for more information. [PR1245686](#)

Chassis Cluster

- On SRX Series devices in a chassis cluster, the Internet Control Message Protocol (ICMP) redirect is not sent from a reth interface for a route advertised through BGP. [PR1249322](#)
- On SRX Series devices in a chassis cluster, when you perform the hold-down-interval configuration the following issues are observed:

- In RG0 hold-down-interval configuration when you use **set chassis cluster redundancy-group 0 hold-down-interval** command, the incorrect value appears as 0 to 1800 seconds but the value should be shown as 300 to 1800 seconds.
- In RG1+ hold-down-interval configuration, RG1+ hold-down-interval range needs to be 0 to 1800 seconds but the value is only available from 300 to 1800 seconds. [PR1104269](#)

Ethernet Switching

- On SRX Series devices, ndra-pool and delegated-pool cannot use the second range. [PR1234243](#)
- On SRX5400, SRX5600, and SRX5800 devices, if **fab 0** and **fab 1** interfaces are changed, the device might drop STP Bridge Protocol Data Unit (BPDU) on RG1+ primary node in transparent mode. [PR1243887](#)

Flow-Based and Packet-Based Processing

- In a chassis cluster, some traffic destined to or sourced from the SRX itself might be dropped when applying application framework services to this traffic while the control plane and data plane are active on different nodes. [PR1210018](#)
- On SRX Series devices, the flowd process might stop when NAT46 session activeness changes from Z-mode operation to active-backup mode at the same time fragment packet belong to that session is being processed. [PR1233879](#)
- On SRX Series devices, during session creation, a memory corruption might occur, which results in the flowd process to stop. [PR1241042](#)
- On SRX5400, SRX5600, and SRX5800 devices, IPsec VPN traffic might be dropped intermittently if **ipsec-performance-acceleration** option is enabled. [PR1245802](#)
- On SRX Series devices with Selective Packet Services configured, multicast traffic might be sent out-of-order by the device. [PR1246877](#)
- On SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800 devices with chassis cluster configured, both IPv4 and IPv6 packets pass through device, when SPU session is aged out, the subsequent packets hits the invalid session. The flowd process might stop and generate a core file. [PR1249891](#)

J-Web

- When you configure J-Web setup wizard through creating new configuration and applying the same does not reflect all the configurations in a router. This displays configuration change alert and ask for committing the configuration. [PR1058434](#)
- On SRX Series device, when more than 25 zone address set entries are configured on the device, the J-Web displays only the first 25 zone address set entries. [PR1247565](#)

- On SRX Series devices, when you add new IP addresses to firewall filter, the J-Web PHP memory does not overflow. [PR1253482](#)
- On SRX Series devices, when you add the static route, the IPv6 option is disabled in J-Web under static routing hierarchy. [PR1254837](#)

Network Address Translation (NAT)

- On SRX Series devices, when NAT is configured, the nsd process might get a memory leak after a NAT config change and commit. [PR1260409](#)
- On SRX Series devices, when source-address match condition for static NAT is configured, the nsd process might stop if the address book contains a lot of addresses. [PR1272477](#)

Network Management and Monitoring

- On SRX3400 and SRX3600 devices, the transmitted bytes value in **show interface queue** displays wrong value. [PR1227762](#)

Platform and Infrastructure

- On SRX Series devices, when a Netconf get-route-information RPC is executed for all routes through the ssh transport session and the session is terminated before all the route information is retrieved, the mgd process and rpd process causes high CPU utilization for an extended period of time. Example of issues caused by high CPU utilization for an extended period are:
 - BGP neighbors hold down timer expire and become ACTIVE
 - OSPF adjacencies reset during database exchange
 - OSPF LSA retransmissions events on neighboring nodes due to missing ACKs
 - LDP sessions time out
 - Non-distributed Bidirectional Forwarding Detection (BFD) sessions being reset due to missing keep alive. [PR1203612](#)
- On SRX Series devices, when you activate a security policy and insert the same policy below the other active policies in the same commit statement, activation works but the insert does not take effect even after a successful commit. [PR1212226](#)
- On SRX Series devices, when you use the **request system software** command along with the **partition** and **validate** options, the current configuration is not validated against the Junos version being upgraded to as part of the upgrade process. [PR1223443](#)
- On SRX Series devices with SRX3K-2XGE I/O cards installed, the interface bandwidth might show wrong value when polling through SNMP OID. [PR1236490](#)

- On SRX Series devices, the secondary node in a chassis cluster environment might stop or go into DB mode, displaying the **panic:rn timer_index_alloc** message. This issue is sometimes observed in a chassis cluster environment with multipoint st0.x interface configured, and the tunnel interfaces flaps according to IPsec idle-timeout or IPsec VPN-monitor. [PR1244491](#)
- On SRX Series devices, the **abnormal timer recovery** error message is displayed frequently in the logs, without any service impact. [PR1260274](#)

User Interface and Configuration

- In Junos OS Release 12.3X48-D45 and earlier, on SRX series devices in chassis cluster, deactivated security policy is moved unexpectedly after new policy when you commit the configuration. [PR1248882](#)

VPNs

- On SRX5400, SRX5600, and SRX5800 devices, the st0 interface global counter statistics is not incrementing and remains zero, although traffic passes through the tunnel sub-interfaces such as st0.0 and st0.1. [PR1171958](#)
- On SRX Series devices, when there are large number of tunnels bound to the same multipoint st0 interface and are using auto next hop tunnel binding, traffic might be sent into incorrect tunnel after tunnel flap or rekey. [PR1226582](#)
- On SRX Series devices, the VPN tunnel and associated secure tunnel (st0) interface go down even though there are active tunnels. [PR1238946](#)
- On SRX Series devices, traffic is lost after adding traffic selector in a IPsec VPN. [PR1249908](#)
- On SRX Series devices, when st0 interface is moved from one routing instance to another routing instance, packet loss is observed. [PR1255593](#)
- On SRX Series devices, if traffic-selector is configured, the IKE redundant gateway failover fails. [PR1270000](#)

Resolved Issues: Release 12.3X48-D45

Application Layer Gateways (ALGs)

- On SRX Series devices, Media Gateway Control Protocol (MGCP) ALG complex calls (group or ACD calls) are not working as expected. [PR1226822](#)
- On SRX Series devices, trivial file transfer protocol (TFTP) ALG logging does not recognize the service TFTP, when both the source port and destination port are not known ports. [PR1232026](#)

- On SRX Series devices, when MSRPC or SUNRPC ALG is used for processing traffic, the flowd process might stop in ALG map entry allocation failure scenarios. [PR1234553](#)

Chassis Cluster

- On SRX1400 device in chassis cluster mode, the replacement of SYSIOC on one of the nodes can cause a split brain condition when that node joins the chassis cluster. [PR1215280](#)
- On Junos Release 12.3X48-D40 and earlier releases, chassis cluster status temporary goes split brain after one of node is rebooted. [PR1217981](#)
- When ICU is used to upgrade a cluster, a longer downtime might be noticed than the one published. This is caused by a timer issue in the sending the GARP packets. [PR1219788](#)
- On SRX Series devices, high CPU on HA secondary node causes jsrpd process scheduling slip. [PR1225219](#)
- On SRX Series devices, primary node HA LED is **amber** even if cluster status is normal and no monitor failures. [PR1230502](#)
- On SRX Series devices, the VRRP advertisements might not be forwarded when packets passes through the switching fabric (SWFAB) link on chassis cluster. [PR1235592](#)
- On SRX Series devices in a chassis cluster, the synchronization monitoring configuration might fail if the following configuration is enabled: **set system encrypt-configuration-files**. The synchronization monitoring configuration failure might result in disabling the secondary node after reboot. [PR1235628](#)

CLI

- On SRX Series devices, the mgd process might stop and generate a core file when **system login user <username-->authentication** statement is configured both in groups and foreground configuration. [PR976970](#)
- On SRX Series devices, the **system commit synchronize** command is not supported. Hence, when you attempt to execute this command, it is not committed because of a configuration lock. [PR1134072](#)

Ethernet Switching

- On all SRX Series devices, when you connect to the device through wireless AP the secure access port incorrectly allows access to the MAC addresses that are not in the list of allowed MAC addresses. [PR587163](#)
- On SRX Series devices, incorrect LACP partner system ID is shown when the AE member link is connected to a different device, this might misguide when you troubleshoot the LAG issues. [PR1075436](#)
- On SRX Series devices in a chassis cluster, if Ethernet switching is configured, because of a timing issue on the swfab interface initialization, the Layer 2 traffic might be dropped after a redundancy group 0 (RG0) failover. [PR1103227](#)

- On SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, and SRX650 devices, when you run **show arp** command in RSI, it might take a long time to complete. [PR1233551](#)
- On SRX Series devices, use prefix-length mask-low or mask-high to configure Neighbor Discovery Router Advertisement (NDRA) pool and delegated pool, and to open jdhcpd trace and generate a core file. [PR1236167](#)

Flow-Based and Packet-Based Processing

- When you run the **show usp flow counters all** command, the output show huge numbers. This does not cause any functional outage. [PR1175469](#)
- On SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800 devices, the BGP might flap if you use reth interface to establish BGP neighbors and the control and fabric links might flap. As a result, the traffic traversing reth interface will be interrupted. [PR1194548](#)
- On SRX Series devices, if the device receives ICMP request or reply with same source IP, destination IP and, sequence number of existing ICMP session that has already received a response, instead of being marked for closure, results in session timeout refreshed. [PR1202432](#)
- On SRX5400, SRX5600, and SRX5800 devices, IPSec VPN traffic might be dropped if the IPSec tunnel in different routing instances, and needs to be routed by routing-instance in a NAT rule. [PR1217583](#)
- On SRX Series devices, the flowd process might stop after committing a configuration of the MTU on an interface with PIM tunnel enabled. For example, after committing MTU, if you set the MTU value to 9192 (maximum allowed by configuration) on the main interface and set the IP MTU to 1500 on all sub interfaces while the PIM is operational. [PR1224808](#)
- On SRX Series devices, if an application with application-ignore is applied for IKE packets (usually, UDP 500 or UDP 4500 in NAT-T scenarios), when the related security policy evaluates the fragmented IKE packets, the first non fragmented IKE packet is not recognized, and is not sent to the iked process, causing the IKE negotiation failure. [PR1227109](#)
- On SRX Series devices, when services-offload is used for multicast handling and fragmented multicast packets are processed the flowd process might stop, generating a core file and the data plane of the processing device gets restarted. [PR1233849](#)
- On SRX5800 device, the output of counters for individual mirror-filters for X2-Mirroring displays 0. [PR1234449](#)
- On SRX Series devices, the output of the **show system auto-snapshot** command is displayed twice. [PR1235859](#)
- On SRX5800 device, a flowd core file is generated when you use X2 traffic monitoring feature between IPsec tunnels. [PR1236253](#)

- On SRX5400, SRX5600, and SRX5800 devices, when you use Internet Key Exchange (IKE) in chassis cluster, memory buffer (mbuf) stall might trigger FPC alarms and RG failover. [PR1236672](#)
- On SRX Series devices in a chassis cluster, the flowd process might stop and generate a core file under the following conditions:
 - IPv6 IPsec VPN tunnel is established
 - NAT is enabled for the IPv6 VPN traffic
 - Performing failover for the VPN traffic related data-plane Redundancy Group (RG). [PR1237311](#)

Forwarding and Sampling

- On SRX Series devices, when the firewall filter is used on GRE interface (gr-), it is applied to packets which are crossing the interface and is not applied to packets which are destined to the device. This issue occurs only in HA mode. In standalone mode the filter works fine. [PR1182267](#)

Interfaces and Routing

- On SRX210 and SRX220 devices with 1x Gigabit Ethernet high-performance SFP configured, the traffic forwarding stops through 1x GE High-Perf SFP. [PR1222648](#)
- On SRX550 device, when you run the **monitor traffic interface** command for the first time after reboot, and then stopped, forwarding in VPLS and Layer 2 circuits might stop. Forwarding is active again when the monitor traffic interface command is enabled, and stops when the **monitor traffic interface** command is disabled. [PR1233209](#)

J-Web

- On SRX Series devices, the high CPU usage on routing engine might occur when you use J-Web. J-Web is slow with displaying contents of logs files under **Monitor-> Events and Alarms->View Events**. [PR1210458](#)
- On SRX Series devices, if an additional application is added in a nested application-set, it removes the application-set in favor of the new application. This issue is seen only in J-Web. [PR1222415](#)
- On SRX series devices, the chassis cluster status is not shown correctly and control link 1 does not show up on J-Web. [PR1226876](#)
- On SRX Series devices, on the J-Web dashboard page, the refresh button does not work properly. [PR1232076](#)
- On SRX1400 device, on the J-Web dashboard page, HA LED shows the wrong color and auto refresh does not work. [[PR1233161](#) and [PR1227908](#)]

Network Address Translation (NAT)

- On SRX Series devices, high memory utilization might be observed on the Routing Engine due to a memory leak in the NSD process, caused by the SNMP polling of NAT statistics. [PR1226337](#)
- On SRX Series devices, when source-address match condition for static NAT is configured, the nsd process might stop if the address book contains a lot of addresses.

Network Management and Monitoring

- On SRX Series devices in a chassis cluster, configure or delete the configuration of **set system no-redirects** and commit, it does not take effect for reth interface. [PR894194](#)
- On SRX5400, SRX5600, and SRX5800 devices in a chassis cluster, constant stream of SPU host mbuf stall messages are seen when the multicast feature is used. [PR1194485](#)

Platform and Infrastructure

- On SRX5600 and SRX5800 devices with NG-SPC, if multicast traffic or Layer 2 flood traffic enters the router through line cards, these line cards might exhibit a lockup, and one or more of their Packet Forwarding Engines corrupt traffic towards the router fabric. [PR931755](#)
- On SRX Series devices, when a Netconf get-route-information RPC is executed for all routes through the ssh transport session and the session is terminated before all the route information is retrieved, the mgd process and rpd process causes high CPU utilization for an extended period of time. Example of issues caused by high CPU utilization for an extended periods are:
 - BGP neighbors hold down timer expire and become ACTIVE
 - OSPF adjacencies reset during database exchange
 - OSPF LSA retransmissions events on neighboring nodes due to missing ACKs
 - LDP sessions time out
 - Non-distributed Bidirectional Forwarding Detection (BFD) sessions being reset due to missing keepalives. [PR1203612](#)
- On SRX5400, SRX5600, and SRX5800 devices, the log message **Warning! random engine is holding busy** is displayed frequently in `/var/log/messages`. [PR1233408](#)
- On SRX650 device, when you run **show arp** in Request Support Information (RSI), the execution of the command might take a long time. [PR1233551](#)
- On SRX240 device, the abnormal reboot results in `/cf/var` does not get mount correctly, causing multiple core files to be generated during device boot up. [PR1237237](#)
- On SRX Series devices with J-Flow v9 sampling is configured. After the packets are sampled, capture all the flow record packets. The value of **SrcMask, DstMask, srcas, dstas, snmp_index** for

incoming/outgoing interface is incorrect within the captured frames. The IPv4 flow and IPv6 flow have the same issue. [PR1241965](#)

Routing Policy and Firewall Filters

- On SRX Series devices, when there is at least one policy using the range address in a zone, the nsd process might stop after running the **show security shadow-policies** command. [PR1232736](#)

Routing Protocols

- On SRX Series devices, in an OSPF routing scenario with Not So Stubby Area (NSSA) configuration, the NSSA router imports an external route and generates a type-7 Link-State Advertisement (LSA), the Area Border Router (ABR) receives and translates this LSA to type-5 LSA. If the type-5 LSA-id clashes with the IP address on the local router in the OSPF area, when you "commit" the configuration, routing protocol process might stop. [PR963814](#)
- On SRX Series devices, in the subscriber management environment, a subscriber login and logout might cause the rpd memory leak of 8 bytes. [PR1011825](#)
- On SRX Series devices when jhpcpd creates a binding, a permanent entry in the Address Resolution Protocol (ARP) table is added for that IP address. When you disable the service, the entry in the ARP table is not cleared and can cause issues later. This issue introduces a check at commit, and informs that there are still entries present and needs to be cleared before you stop the service. [PR1228493](#)

Unified Threat Management (UTM)

- Starting with Junos OS release 12.3X48-D40, virus files more than 32 KB detection fails when the UTM anti-virus feature is used. [PR1225771](#)

VPNs

- When you use non-reth interfaces in a chassis cluster during traffic that needs to be encapsulated in GRE and then sent over an IPsec tunnel, the other peer might notice that the ESP packets are being sent by the device with incorrect sequence numbers. [PR1169537](#)
- On SRX550 device acting as VPLS local switch, when you disable the interface connected to a layer 3 device which is attached to the VPLS routing instance, they start to have a loop behavior and the switch connects to other interface of the VPLS routing instance. The switch updates MAC table to all MACs using the interface attached to the VPLS routing instance. On the device, the VPLS interfaces does not enable redirect, causing split-horizon failure. [PR1223280](#)

- On SRX Series devices, when there are large number of tunnels bound to the same multipoint st0 interface and are using auto next hop tunnel binding, traffic might be sent into incorrect tunnel after tunnel flap or rekey. [PR1226582](#)

Resolved Issues: Release 12.3X48-D40

Application Layer Gateways (ALGs)

- On all SRX Series devices, when RSH ALG is enabled manually, RSH ALG receives a message whose stderr port is 0, RSH ALG will drop packets and will not open gate for it. When encounter the issue, please disable RSH ALG. [PR1196530](#)

Authentication and Access Control

- During firewall HTTP or HTTPs pass-through authentication, the device incorrectly remove the preceding colon in the password string. Due to this the authentication fails and the authentication entry cannot be created in case there is preceding colon in the password string. [PR1187162](#)

Chassis Clustering

- On SRX1400 Series devices in a chassis cluster with a SYSIO board of hardware revision 20 or revision 18, the first control link on port ge-0/0/10 might not come up immediately after an ungraceful power-off and power-on. [PR1166549](#)
- In the chassis cluster, the fabric link flaps randomly after upgrading to the 12.1X46 and onwards. [PR1197954](#)
- On all SRX Series devices with dual fabric link chassis cluster, one of fabric link sometimes shows as down after RGO failover or node reboot even there is fabric probe on the link. [PR1207919](#)

Flow-Based and Packet-Based Processing

- When issuing the following command on the **show security flow session summary**, the bfd sessions might flap. [PR1198266](#)
- On SRX Series devices in a chassis cluster, high CPU usage on data-plane might occur when **ipsec-performance-acceleration** is enabled. [PR1097278](#)
- On all SRX Series devices, when configuring white-list for security screen, it might cause memory corruption in Jtree, which results in the flowd process to stop. [PR1172844](#)

- When AppQoS enabled, some of sessions hit appqos policy will not be created properly at high memory utilization. As a result, packet related the session will drop. [PR1190889](#)
- On SRX Series devices, prior to Junos OS Release 12.3X48-D70 all formats in ISO8601 such as **2016-06-06T00:31:52-07:00** are not supported. [PR1198521](#)
- On SRX Series devices, RSH client communicates with RSH server. RSH ALG is enabled. RSH client transfers file to RSH server. Some last packets from the RSH server are not forwarded to the RSH client. [PR1202773](#)

Infrastructure

- On SRX5400, SRX5600, and SRX5800 devices, SNMP traps are not sent when the ECC double error occurs. [PR1185158](#)
- When you plug out and re-plug the modem at CBA750B/CBA850, leading to CBA750B/CBA850 MIB tree change. This might cause the SRX Series device to not get the modem information from the expected MIB node. In such scenarios, the device will display the following modem information: "Connection status: Down" and all counters are set to zero by default. This is a status show problem, data link might still work. To fix this problem, just reboot the CBA750B/CBA850. CBA750B/CBA850 will rebuild the MIB tree and SRX Series device can get the information correctly. [PR1187675](#)

Interfaces and Routing

- The Software-NH value increases and causes the traffic outage. [PR1190301](#)
- On SRX210 and SRX220 devices, ARP request is not sent by ge-0/0/0 interface with the **family ethernet switching** configured. [PR1206017](#)

Intrusion Detection and Prevention (IDP)

- On all SRX Series devices a yellow alarm might be reporting on the craft display after a reboot when using EWF or IDP licenses. [PR1156185](#)
- On SRX Series devices, you cannot compile the IDP policy when LSYS idp-policy-combined is created. [PR1187731](#)
- On all SRX Series devices, the flowd might stop on both the nodes after the IDP database update and causes the traffic to be interrupted. [PR1202319](#)

J-Web

- Error messages are seen on J-Web when adding a custom-applications setting with term. [PR1183037](#)

- On all SRX Series devices, after using J-Web it might occur that the CPU utilization on the routing-engine will stay high and does not recover. [PR1201267](#)
- On SRX Series devices in a chassis cluster, J-Web does not show correct chassis cluster status in the following page J-Web: **Monitor->System view->cluster** status. [PR1208901](#)

Network Address Translation (NAT)

- On all SRX Series devices, while using source-based NAT with egress interface translation, upon egress interface IP address change, the current NAT sessions might not be removed until the session is aged-out. Traffic loss will occur while the traffic attempts to pass on the sessions using the old egress interface NAT IP. [PR1201415](#)
- The flowd process (responsible for traffic forwarding in SRX Series device) might stop and generate core files while committing a NAT configuration with minor change first and then commit a major change. [PR1221427](#)

Network Management and Monitoring

- Constant stream of **SPU host mbuf stall** messages are seen when the multicast feature is used in the SRX chassis cluster. [PR1194485](#)
- When you run show system license usage command it might show invalid scale-subscriber license on new RG00 master node after RG0 failover. This is only a cosmetic issue and there is no impact to function/performance/traffic. [PR1197211](#)
- On SRX devices, **set system time-zone** configuration does not affect time stamp in stream mode security log. [PR1203833](#)

Platform and Infrastructure

- On SRX5000 device with SPC2 cards, flowd core files might occur under high traffic load related to a corrupted CPU stack. [PR1183333](#)
- When an upgrade is attempted to version 12.3X48 and event scripts are enabled in configuration, the upgrade might fail with the reason "validation failed". [PR1189403](#)
- A vulnerability in IPv6 processing has been discovered that might allow a specially crafted IPv6 Neighbor Discovery (ND) packet to be accepted by the router rather than discarded. The crafted packet, destined to the router, will then be processed by the routing engine (RE). A malicious network-based packet flood, sourced from beyond the local broadcast domain, can cause the Routing Engine CPU to spike, or cause the DDoS protection ARP protocol group policer to engage. When this happens, the DDoS policer might start dropping legitimate IPv6 neighbors as legitimate ND times out. Refer to JSA10749 for more information. [PR1191838](#)

- On SRX5400, SRX5600, and SRX5800 devices, the device stops working after broadcast storm and this situation lasts for nearly 12 hours. [PR1192536](#)
- Secret data such as some encrypted passwords was displayed in RSI by **show configuration | except SECRET** command in RSI. [PR1192579](#)
- On SRX Series devices, if there are two or more IP Monitoring configured, and they operate the same IP prefix, then unexpected behavior with IP Monitoring might occur, such as false negative. [PR1192668](#)
- With pass-through authentication in SRX devices, Firewall client access destination server by old browser (browser like MS-IE4/MS-IE5), the flowd process might stop on all SRX Series devices when pass-through http traffic which matches the fwauth-policy. [PR1203294](#)
- Packets passing arriving on MPLS LSP may be sent out-of-order post SRX processing. [PR1213699](#)

Routing Policy and Firewall Filters

- On all SRX Series devices, there might be a traffic outage if failover happens between node 0 and node 1 and the nsd process fails to read the security policies from the configuration file. [PR1182591](#)
- On all SRX Series devices, when range-address is configured on an address-book and invoked by a security policy, an abnormal memory access might occur, which causes the flowd process to stop. [PR1196122](#)

System Logs

- On all SRX Series devices, two new fields **src-nat-rule-type** and **dst-nat-rule-type** are added for session logging providing ability to distinguish duplicate named rules. [PR1041685](#)

Unified Threat Management (UTM)

- On SRX Series devices, when UTM, Security log, or Advanced Anti-Malware Service is used, in a rare condition, a memory corruption might occur on data-plane, which results in the flowd process to stop. [PR1154080](#)
- On SRX Series devices, in chassis cluster, utmd process might generate a core file on the secondary node, even though UTM features are not configured. This issue has no impact on traffic flow. [PR1194713](#)
- On SRX Series devices, after using the UTM services, anti-virus or anti-spam for some time, DNS lookups might start to fail and the UTM service resorts to fallback. [PR1207651](#)

VPNs

- On SRX Series devices, in the IPsec VPN with certificate based authentication in very rare occasion with newly generated key-pair, the authentication may fail during IKE negotiation. [PR1146279](#)
- When using P2MP IPsec VPN tunnels with Dynamic routing over tunnel, a ksyncd core may be encountered after RG0 failover on previous RG0 primary node, if dynamic routing is removed from VPN tunnel prior to RG0 failover. [PR1170531](#)
- Customer using IKEv2 and aggressive mode for several gateways, where the external interfaces are the same, after some time of establishment, when trying to renew phase one, logs will show that the VPN will try to use the information of the last established VPN to renew this one, leading to a failure to reestablished the IPsec VPN. [PR1187988](#)
- On SRX Series devices, after restarting the chassis FPC which the Group VPN external-interface anchored on, the GVPN member IPsec SA is unable to recover. [PR1198089](#)
- On SRX Series devices, when **set system no-compress-configuration-files** is configured, the IPsec tunnels will stay down after a reboot or cluster failover. [PR1203723](#)
- On SRX Series devices, when **set system no-compress-configuration-files** is configured, the IPsec tunnels will stay down after a reboot or cluster failover. [PR1207020](#)

Resolved Issues: Release 12.3X48-D35

Application Layer Gateways (ALGs)

- On SRX Series devices, the mapping of the Microsoft Remote Procedure Call (MS RPC) universally unique identifier (UUID) to the object identifier (OID) does not associate the security zone information. MS RPC data traffic matching a specific UUID might not be searched for the correct security policy. As a result, MS-RPC data traffic might be dropped. [PR1142841](#)
- On SRX Series devices, MSRPC ALG cannot decrypt the encrypted EPM messages authlevel **RPC_C_AUTHN_LEVEL_PKT_PRIVACY** and drops the encrypted EPM messages. New behavior will bypass such encrypted messages and generate a syslog message. [PR1192477](#)

Chassis Cluster

- On SRX1400 devices in a chassis cluster with a 10-Gigabit Ethernet SYSIO board of hardware revision 20, the first control link on port ge-0/0/10 might not come up after an ungraceful power-off and power-on. [PR1166549](#)

- On all SRX Series devices in chassis cluster mode, when some configuration needs to be changed, after issuing the CLI **commit confirm** (the time parameter value can be between 1-65535) and **commit** command on the primary node, the secondary node does not commit. [PR1171366](#)

Flow-Based and Packet-Based Processing

- On SRX Series devices with IOC II cards installed and np-cache feature enabled, low performance might be seen when fragmented traffic is present. [PR1193769](#)

Network Address Translation (NAT)

- On SRX Series devices, when NAT with port-block allocation (PBA) is configured, the CPU is utilized at the optimum level and it affects the protocols such as LACP. This issue might cause temporary network instability. [PR1172347](#)

VPNs

- On SRX Series devices, in some cases, a memory leak might occur when using route-based or policy-based VPN and peer attempting multiple phase 2 connections with different proxy IDs. [PR1174974](#)
- On SRX Series devices, after the command **chassis fpc restart**, the GVPN member IPsec SA is unable to recover. [PR1198089](#)

Resolved Issues: Release 12.3X48-D30

Application Layer Gateways (ALGs)

- On SRX Series devices with the MS-RPC ALG enabled, in heavy MS RPC traffic, ALG traffic might fail because of the ASL groups being used up. [PR1120757](#)
- On SRX Series devices in a chassis cluster, when SCCP traffic is processed by the SCCP ALG, the flowd process might stop. [PR1154987](#)
- On SRX Series devices with the H.323 ALG enabled, in a rare condition, if a gatekeeper sends a RAS gatekeeper confirm (GCF) packet that contains an extension with an authentication mode header, the H.323 ALG will drop the GCF packet. As a result, the register of H.323 client to gatekeeper will fail. [PR1165433](#)

Chassis Cluster

- On all SRX Series devices in chassis clusters, when you configure the MAC address on the reth interface using the **set interfaces reth* mac *** command, all reth member interfaces use the manually specified MAC address. When you use the **deactivate interfaces reth* mac** command, the reth interface will change to the default MAC address, but the reth member interfaces will remain in the manually specified MAC address. This scenario causes traffic issues on the reth interface. [PR1115275](#)
- On SRX Series devices in a chassis cluster, the Link Layer Discovery Protocol (LLDP) is not supported on reth interfaces. [PR1146382](#)
- On SRX Series devices in a chassis cluster, if the control plane RG0 and data plane RG1+ fail over simultaneously, the reth interface on the new master node might send Generic Attribute Registration Protocol (GARP) packets in an unexpected delay of approximate 11 seconds. This causes a temporary traffic outage. [PR1148248](#)
- On SRX Series devices in chassis clusters, after rebooting the whole system, the directed connected route for a disabled reth interface or logical interfaces might remain in the active state in the forwarding plan because of a timing issue. This issue results in traffic being forwarded to the disabled reth or logical interface. [PR1149857](#)

Class of Service (CoS)

- On all multi-thread SRX Series devices, when an interface is down, a timing issue in which one thread releases the interface resource (because the interface is down), but another thread tries to access this interface resource might occur, which results in a flowd process to stop. [PR1148796](#)

CLI

- On SRX Series devices, the **system commit synchronize** command is not supported. Hence, when you attempt to execute this command, it will not be committed because of a configuration lock. [PR1134072](#)

Flow-Based and Packet-Based Processing

- On SRX Series devices, if a device is configured as a DHCP relay using the `jdhcpd` process, the option 82 is not supported. The DHCP discover or bootp packets containing option 82 are dropped. [PR979145](#)
- On SRX Series devices acting as a rendezvous point (RP), when the device receives successive PIM register packets, only the first one will be de-encapsulated and sent out; the subsequent PIM register packets are dropped. The multicast data packets might also drop because reverse path forwarding check failure occurs during the multicast routing entry installation sequence. [PR1114293](#)
- On SRX Series devices, IPv6 host-inbound traffic destined to `xnm-ssl` and `xnm-clear-text` services will be dropped even if `xnm-ssl` and `xnm-clear-text` are permitted in host-inbound traffic. [PR1147446](#)

- On SRX Series devices with IPsec VPN configured with VPN session affinity enabled, the VPN traffic might loop between the central point and the SPU because of a timing issue. This issue might cause a CPU spike on the central point and the SPU. [PR1154649](#)
- On SRX Series devices, when using MS Windows as a client and downloading a large file through the antivirus feature, the download speed might be suboptimal when the client throttles the incoming flow by decreasing its TCP window size. [PR1155228](#)

General Routing

- On SRX Series devices acting as a DHCP server, the DHCP binding with a lease time configured might never expire, which will exhaust all IP addresses of the DHCP pool. [PR1050723](#)
- On an SRX Series device configured as a DHCP server, the device will not send DHCP option 125 unless the DHCP client requests it. This behavior does not comply to the RFC definition. According to RFC 3925, the DHCP server should send option 125 without the client's request. [PR1116940](#)

Intrusion Detection and Prevention (IDP)

- On SRX Series devices, when the IDP SSL inspection feature is enabled and processes traffic, in a race condition of multiple threads updating a reference count concurrently, corrupted data might be created and cause the idpd process to stop. [PR1149604](#)

Interfaces and Chassis

- On SRX Series devices with enhanced fan trays equipped, the **Fan Tray Unable to Synch** alarm might be seen. [PR1013824](#)
- If a configuration pertaining to a 3G interface is present and if a 3G modem is not connected to the device, Junos OS might try to access the 3G thread. As a result, the device might stop when the device cannot find the 3G thread. [PR1151904](#)

J-Web

- On SRX Series devices, multiple vulnerabilities exist in J-Web input handling that might lead to cross-site request forgery (CSRF) issues or cause a denial of J-Web service (DoS). The CSRF vulnerabilities might allow malicious content on third-party websites to launch unauthorized access and actions against J-Web through an administrative user's browser. [PR1085861](#)

Network Address Translation (NAT)

- On SRX Series devices, when a routing instances name is configured with 32 characters or more for a virtual router, the interface that is configured with NAT proxy-arp in that virtual router does not respond to any ARP request. [PR1164600](#)

Platform and Infrastructure

- On SRX Series devices in a chassis cluster with dual control links, if the first control link (em0) goes down, the master Routing Engine does not send the IP traffic to the remote node. This means that if, for example, redundancy group 0 (control plane) is primary on one node and redundancy group 1 (data plane) is primary on another node, any IP traffic originated on the Routing Engine will not be passed out. [PR1051535](#)
- On SRX Series devices, there are multiple vulnerabilities in cURL and libcurl. For more information, refer to KB <https://kb.juniper.net/JSA10743>. [PR1068204](#)
- On SRX5600 and SRX5800 devices with a SRX5K RE-13-20 Routing Engine, in dual control link configuration, the second control port - em1 link remains down when the Routing Engine installed in slot 1 is installed with Junos OS Release 12.1X47 or later. [PR1077999](#)
- On SRX Series devices, the chassis cluster LED changes to amber after RG0 failover, but the CLI indicates it is green. [PR1085597](#)
- On SRX Series devices, the file descriptor (FD) might leak on the httpd-gk process when the system fails to connect to the mgd process management socket. [PR1127512](#)
- Memory leaks on the mib2d process are seen during polling of SNMP OID .1.3.6.1.2.1.54.1 (SYSAPPLMIB). [PR1144377](#)
- The CLI **set system autoinstallation** command configures unit 0 logical interface for all the physical interfaces that are up, which might result in failure of the CLI commands that do not allow unit logical interface configuration. This issue might cause the dcd process to stop, and the interface-related configurations to be installed incorrectly. [PR1147657](#)
- On SRX Series devices, when using J-Web, the mgd process might hang which might result in high CPU usage on the Routing Engine. [PR1155872](#)

Routing Policy and Firewall Filters

- On SRX Series devices, duplicate address-book entries used in the same security policy might cause policy out-of-sync messages to be reported between the Routing Engine and the Packet Forward Engine. [PR1161539](#)

Services Applications

- On SRX Series devices, the name of the ICMP6 big packet is changed to **junos-icmp6-packet-too-big** instead of **junos-icmp6-packet-to-big**. [PR917007](#)

Unified Threat Management (UTM)

- On SRX Series devices, if a custom routing instance is used to connect the server of UTM enhanced Web filtering, when the server is configured using an IP address (**set security utm feature-profile web-filtering juniper-enhanced server host *.*.***), an incorrect routing instance is used to connect the server. When the server is configured using a URL, an incorrect routing instance might be used to connect the server if the Web filtering configuration is changed. As a result, the connection fails. [PR1159827](#)

VLAN Infrastructure

- On SRX Series devices, when the device sends ACK packets to the source, the source and destination MAC addresses are built in a reverse direction this might affect the forwarding traffic. [PR1140242](#)

VPNs

- When using the IKEv2 configuration payload feature, the DNS server value is not propagated to the IKEv2 client. [PR1064701](#)
- On SRX Series devices in a chassis cluster, when RG0 failover occurs, the pp0 interface might flap. If an IPsec VPN tunnel is established using a pp0 interface as the external interface, due to a timing issue, the pp0 interface flapping might cause the VPN tunnel session and the IPsec security association (SA) installed in the data plane to be deleted. However, the IKE or IPsec SA installed in the Routing Engine will still remain, which causes a VPN traffic outage. [PR1143955](#)
- On SRX5400, SRX5600, and SRX5800 devices in a chassis cluster, when IPsec VPN is established using AES-GCM (included in the Suite B and PRIME cryptographic suites), an IPsec VPN-related data plane redundancy group (RG1+) failover might cause VPN tunnel renegotiation. [PR1153214](#)

- On SRX Series devices acting as a key server in a group VPN scenario, the flowd process might stop. [PR1164668](#)
- On SRX Series devices, GVPN members use a new security parameter index (SPI) for packet encryption before the intended time. [PR1171573](#)

Resolved Issues: Release 12.3X48-D25

Application Layer Gateways (ALGs)

- On all SRX Series devices, the RSH ALG does not inspect the legality of the control message. Hence the malformed messages are bypassed. However, by default, the RSH ALG is disabled on Junos OS releases containing this fix. [PR1093558](#)
- On all SRX Series devices with the H.323 ALG enabled, if dual NAT (the packets in the same call receive different NAT rules bidirectionally) is enabled, then the destination NAT for the payload is skipped during ALG processing. For example, the address payload in the H.225 gatekeeper confirm packet is not translated by the H.323 ALG. [PR1100638](#)
- On SRX Series devices with DNS proxy enabled, any configuration change related to DNS service triggers the named process restart. The configuration at the **system services dns dns-proxy hierarchy** level might not be loaded after the named process restart because of a timing issue. [PR1113056](#)
- On SRX Series devices, in J-Web, the configuration of RSH and SQL ALG status is wrong and is inconsistent when compared with the actual status confirmed by the CLI. [PR1128789](#)

Chassis Clustering

- On SRX Series devices in a chassis cluster, the G-ARP is not sent with a static MAC address when chassis cluster failure occurs. [PR1115596](#)
- On SRX5400, SRX5600, and SRX5800 devices in a chassis cluster with SRX5K-MPC (IOC2), SRX5K-MPC3-100G10G (IOC3), or SRX5K-MPC3-40G10G (IOC3) installed, when VLAN tagging is configured on the reth interface and LACP is enabled, and if the logical reth interfaces with VLAN tagged are configured within separate security zones, then the LACP protocol fails. [PR1128355](#)

Flow-Based and Packet-Based Processing

- On SRX5400, SRX5600, and SRX5800 devices, when the SPU works in high stress mode, the internal event queue can be full, and an event can be lost. There is no retransmission mechanism for this internal event, and the connection enters a “session stuck” state. The session that hangs is recovered by the upper layer applications. For example, when the TCP session log module is hung, you cannot send any log messages. After 30 seconds, the log module detects this condition and restarts the new connection to send the log message. However, if the UDP session log module is hung, you can still send the log message. [PR1060529](#)
- On all SRX Series devices, if equal-cost multipath (ECMP) routing is configured, in a race condition of ECMP route updating, the flowd process might stop. [PR1105809](#)
- On SRX Series devices with IPsec VPN configured, if traffic is transmitted from one VPN tunnel to another VPN tunnel, and these two VPN tunnels are anchored on different SPUs, then this VPN traffic might be forwarded in a loop between these two SPUs. [PR1110437](#)
- On all SRX Series devices, a flowd process might stop when dynamic routing with ECMP is in use. [PR1125629](#)
- On all SRX Series devices with multi-threaded forwarding engines that have the **tcp-session strict-syn-check** feature enabled, the initial packets of a TCP session might be dropped due to a race condition. [PR1130268](#)
- On SRX Series devices, in a rare condition, SPUs might run into a deadlock situation, which results in the flowd process to stop. [PR1132059](#)
- On SRX Series devices, traffic drops because of flow skipping source NAT before handling session-affinity for IPsec tunnel traffic. [PR1137926](#)

Hardware

- On SRX Series devices, model numbers of Restriction of Hazardous Substances (RoHS) compatible power entry modules (PEMs) are not displayed when you run the **show chassis hardware models** command. [PR1138773](#)

Interfaces and Chassis

- On SRX Series devices in a chassis cluster, the set protocols lldp interface all command configures the LLDP protocol even on the reth interface. However, the reth interface does not support this feature. [PR1127960](#)
- On SRX Series devices, when you modify a security zone that has many interfaces (for example, when adding or deleting an interface in such a zone), an abnormally high CPU load might occur upon commit. [PR1131679](#)

- On SRX240, SRX550, and SRX650 devices, after a system reboot or disabling and then enabling a Layer 2 reth interface, the reth interface might not work even when the state of the interface is shown as **up**. [PR1137395](#)

Intrusion Detection and Prevention (IDP)

- On SRX Series devices with IDP SSL inspection enabled, traffic with an RSA key size more of than 2000 might cause high CPU usage and performance degradation on the data plane. [PR1125387](#)

Layer 2 Ethernet Services

- On all SRX Series devices, if the device acts as a DHCP server using the jdhcpd process and if the DHCP client sends a discover message with a requested IP address, then the authd process uses the requested IP address to find the pool with priority. This causes the device to assign an IP address from an incorrect DHCP pool to the DHCP client when there is a DHCP pool that shares the same subnet with the requested IP address. However, it is not the expected pool of the DHCP client. [PR1097909](#)
- On all SRX Series devices, if both the DHCP client and the DHCP server (using the jdhcpd process) are enabled, then changing the DHCP-related configuration might cause the jdhcpd process to exit unexpectedly. [PR1118286](#)

Network Address Translation (NAT)

- On SRX Series devices in a chassis cluster, when NAT with port-block allocation is configured, duplicate system log messages might be generated for each port-block allocation and release. [PR1118563](#)
- On SRX Series devices when PBA NAT is configured, the last port-block might be released too early, without considering the configured active-block timeout value. [PR1146288](#)

Platform and Infrastructure

- When you run the commit confirmed command and if the final commit is issued just a few seconds prior to the scheduled roll back, then the system tries to commit and rollback at the same time, which leads to a configuration database corruption issue. [PR994466](#)
- Cross-site scripting (XSS) vulnerability might still be seen after you run the Qualys Scan when HTTP traffic with the host header. [PR1076799](#)

- On SRX210 or SRX220 devices in a chassis cluster, if a VLAN interface is configured as the interface of a JDHCP server, the **DHCPDISCOVER** message is displayed. This results in JDHCP server function failure. [PR1088134](#)
- On SRX Series devices in a chassis cluster, when ungraceful shutdown of the primary node occurs, the PPPoE connection goes down and does not get reestablished. When the primary node that was shut down reboots and joins the cluster, the PPPoE connection gets reestablished. [PR1144078](#)

Routing Policy and Firewall Filters

- On all SRX Series devices, file descriptor leak might be seen during the nsd process, when polling the following OIDs through SNMP:
 - jnxLsysSpCPSummary
 - jnxLsysSpSPUSummary
 - jnxLsysSpCPUEntry
 - jnxLsysSpCPUTable

Unified Threat Management (UTM)

- When the device is configured using HTTPS for UTM antivirus pattern update, the device incorrectly sends the polling packets on TCP port 80, which results in route lookup failure and pattern update failure. [PR1133283](#)
- On all SRX Series devices in a chassis cluster with UTM configured, in a rare condition, the reth interface might go down, and this might cause the flowd process to stop. [PR1136367](#)
- On all SRX Series devices, the Enhanced Web Filtering (EWF) module is bypassed if the TCP session starts with a TCP SYN packet that has multiple flags turned on in its header (for example, SYN+ECN+CWR). [PR1144200](#)

User Firewall

- On all SRX Series devices with integrated user firewall configured, if there are more than 1500 users configured in one group on the Active Directory (AD) server, the device might get into an infinite authentication query loop situation. This situation results in high CPU usage on the AD server, and all subsequent user authentications might fail. [PR1086348](#)
- On all SRX Series devices, configurations attempting to use **ssl-termination-profile** for HTTPS traffic handling using user firewall authentication are ignored. [PR1140115](#)

VPNs

- In group VPN setups, memory might leak during the gksd and gkmd processes. [PR1098704](#)
- On SRX5400, SRX5600 and SRX5800 devices, the active FTP data session fails if traffic selectors are configured for IPsec VPN. [PR1103948](#)
- On all SRX Series device, if there are lots of IPsec VPNs configured, any configuration committing related to IPsec VPN might cause a pause in the kmd process, which might cause Dead-Peer-Detection (DPD) timeout and VPN tunnel renegotiation. [PR1129848](#)
- Downloading a large CRL over LDAP fails in some conditions, causing high CPU usage on the Routing Engine. [PR1130164](#)
- On SRX Series devices acting as a hub in a hub-and-spoke VPN scenario, after a system reboot, some IPsec VPN tunnels might not be established. [PR1132925](#)
- Dynamic VPN cannot connect, and the error **fail to get HTTP Response** appears in the Pulse client.

Resolved Issues: Release 12.3X48-D20

Application Layer Gateways (ALGs)

- On all SRX Series devices, with the default configuration, the SQL ALG is disabled. If you require SQL ALG configurations, you need to enable the SQL ALG. [PR1077810](#)
- On all SRX Series devices with NAT and SIP ALG enabled, the NOTIFY message might incorrectly arrive earlier than the 200 OK REGISTER message, which will disrupt the state machine of the REGISTER message. The subsequent 200 OK REGISTER messages are dropped and the persistent NAT entry is not refreshed, causing the persistent NAT entry to expire. As a result, the IP address in the payload of the SIP message is not translated and the SIP call fails. [PR1064708](#)
- On all SRX Series devices with NAT configured, a memory overwrite issue occurs when the scaling RAS or H.323 traffic passes through the device and the device fails to perform NAT for RAS or H.323 traffic. As a result, the flowd process might stop. [PR1084549](#)

Authentication and Access Control

- On SRX Series devices with firewall authentication configured, an authentication entry leak on the data plane occurs when an authenticated user tries to re-authenticate. As a result, firewall authentication will not allow anymore authentication entries to be created. [PR969085](#)

Chassis Cluster

- On SRX Series devices, when GPRS tunneling protocol version 2 (GTPv2) is configured, GTPv2 might fail to create control sessions. [PR1029284](#)
- On SRX1400, SRX3400, or SRX3600 chassis cluster, if the chassis cluster fabric ports are connected through a switch, some random packets might come into the chassis cluster fabric ports. These packets are interpreted as chassis cluster packets (such as real-time objects) and are forwarded to an invalid SPU. For example, the packets are forwarded to a SPU that does not exist (depending on the interpretation of the invalid packets). The invalid chassis cluster packets cannot be forwarded to the invalid SPU. Hence, the packets will be queued on a certain network processor. When the network processor is full, all data traffic will be blocked on the ports associated with that network processor. [PR1042676](#)
- On all SRX Series devices in a chassis cluster, if sampling is configured with the **input** option on an interface, the non-first fragmented packets are dropped on the secondary node. This occurs when the fragmented packets enter the interface, traverse through the fabric interface, and finally are sent out through the secondary node (z mode). [PR1054775](#)
- On SRX5400, SRX5600, and SRX5800 devices with the SPC2 (SRX5K-SPC-4-15-320) installed, after the control plane (RG0) failover, if the RG0 and data plane groups (RG1+) are active on different nodes, then the primary Routing Engine might drop the connection with the remote SPUs (the SPUs reside on an another node, which is the Routing Engine in a secondary state). As a result, traffic outage occurs. [PR1059901](#)
- On SRX5600 and SRX5800 devices, traffic outage might occur with hardware errors (IA PIO errors). When the devices are configured in a chassis cluster, the hardware errors (IA PIO errors) do not trigger RG1+ failover. This fix is used to raise an FPC minor alarm to trigger the RG1+ to switch over for a chassis cluster. [PR1080116](#)
- On SRX5400, SRX5600, and SRX5800 devices, the warning message **Warning: If you enable this feature on 40x1GE IOC, please refer to manual for the limitation** refers only to the 40x1GE IOC card; instead it should refer to all IOC cards for SRX5400, SRX5600, and SRX5800 devices. [PR1082396](#)
- On all SRX Series devices, all interfaces of the RG0 secondary node go down when the connection between the kernel of the primary node and the ksyncd of the secondary node fails. This occurs because of the memory leak in the shared-memory process (shm-rtssdbd). [PR1084660](#)
- On all SRX Series devices in a chassis cluster, when you disable the member interface of a redundant Ethernet (reth) interface and if the interface disabling action causes redundancy group failover (for example, the only member interface under the reth interface on the primary node is disabled or the

number of operating member interfaces under the reth LAGs interface on the primary node falls below the configured value of minimum-links), then the reth interface will flap. [PR1111360](#)

Class of Service (CoS)

- On all SRX Series devices, the CoS rewrite rules do not work for VPN traffic if the rules are configured with **loss priority high**. This occurs when the packets are reinjected into the IPsec tunnel encapsulation process. [PR1085654](#)

Dynamic Host Configuration Protocol (DHCP)

- On SRX Series devices with a DHCPv6 client configured, when the device tries to obtain an IPv6 address through the DHCPv6 prefix delegation, the device forms an incorrect IPv6 address format. As a result, the IPv6 address allocation fails. [PR1084269](#)

Flow-Based and Packet-Based Processing

- On SRX Series devices configured with chassis cluster and logical systems (LSYS), when the session number is close to the configured LSYS session limit, sessions might not be successfully created on the secondary node. The sessions will be created on the backup flow SPUs, but not on the central point. As a result, the backup flow SPUs will keep retrying until the SPUs are successful. When this situation continues, the session limit on the secondary node's SPU will reach the maximum limit value and this will affect the new session creation.

NOTE: The number of sessions on the secondary node SPU is usually higher than on the primary node SPU. [PR1061067](#)

- On SRX Series devices, the flowd process might stop when the multicast traffic processes the route lookup failure. [PR1075797](#)
- On SRX240, SRX550, and SRX650 devices with integrated user firewall authentication configured, when you attempt to remove the user entry from the authentication table, the flowd process might stop. [PR1078801](#)
- The link-local packets for IPv4 (169.254.0.0/16) and IPv6 (fe80::/10) addresses are dropped. There is no configuration option available to change this behavior and forward the link local packets. [PR1078931](#)
- On all SRX Series devices with source NAT configured, the ICMP error packets with 0 value of MTU might be generated on the egress interface when the packets fail to match the NAT rules. [PR1079123](#)
- On all SRX Series devices, if there are any configuration changes made to the interface (for example, when you add a new unit for an interface), an internal interface-related object will be freed and reallocated.

However, in a rare condition, some packets queued in the system might refer to the freed object, causing the flowd process to stop. [PR1082584](#)

- On all SRX Series devices with integrated user firewall configured, when the user group is specified under the **source-identity** match criteria even though the valid user entry exists in the **active-directory-authentication-table**, the traffic fails to match the security policy for the user who belongs to that user group. [PR1084826](#)
- The flowd process might stop because of a 64-bit unaligned memory access. [PR1085153](#)
- On all SRX Series devices, if 1:1 sampling is configured for J-FLOW, and when the device processes high volume traffic, a race condition of an infinite loop of J-Flow entry deleting might be encountered, which results in the flowd process stop. [PR1088476](#)
- On all SRX Series devices, if the **inactivity-timeout** value of an application is more than 65,535, only the 16-bit value is used to calculate the **inactivity-timeout** value, which causes the application sessions to expire unexpectedly. [PR1093629](#)
- On all SRX Series devices working in transparent mode, the OSPFv3 packets are dropped when they pass through the device and are inspected by a deep packet inspection (DPI) function. [PR1094093](#)
- The **maximum-sessions** value is not displayed correctly. [PR1094721](#)
- On all SRX Series devices, if Services Offloading is enabled, in certain cases, such as packets flowing on an LAG interface or fragmented packets processing, duplicated packets might be randomly generated and forwarded out of the device. [PR1104222](#)
- In a GRE over IPsec VPN scenario, if VPN is deactivated on one side, the outgoing interface of the GRE session on the other side changes to the default route outgoing interface and does not return to the secure tunnel (st0) interface even when VPN is activated. [PR1113942](#)
- On all SRX Series devices (except the SRX110) in a chassis cluster, when ECMP is configured across the interfaces on both nodes, packets are dropped intermittently. [PR1123543](#)

Infrastructure

- On SRX Series devices with health monitor configured for Routing Engine, the system health management process (syshmd) might stop due to a memory corruption in some rare conditions, such as in the scenario that concurrent conflicting manipulation of the file system occurs. [PR1069868](#)
- On SRX100, SRX110, and SRX210 devices, when you use Sierra Wireless USB 3G modem to connect to the network, Junos Space (or other Network Management devices) might fail to discover the SRX Series devices. This is because the Sierra Wireless USB 3G modem generates a duplicate address that causes the failure. [PR1070898](#)

Interfaces and Chassis

- On SRX100, SRX110, SRX210 devices with 3G or 4G USB cellular modems, sometimes the 3G or 4G connection is unstable and does not reconnect when the connection drops. [PR1040125](#)
- On SRX550 and SRX650 devices, when you insert an SFP into a GPIM, the self-traffic is delayed while the chassis reads the SFP data. This might cause a flap for protocols with aggressive timers, such as BFD or BGP. [PR1043983](#)
- When the underlying interface of the PPPoE interface is a reth interface, there is a delay of 10 seconds in displaying the PPPoE interface information when you run the **show interfaces pp*.*** command. As a result, a slower response time for the SNMP command related to the PPPoE interface is also observed. [PR1068025](#)
- If an aggregated Ethernet interface (ae) is configured as a Layer 2 interface, traffic might only be forwarded on one child interface of the ae interface. [PR1074097](#)
- The flowd process might stop when the port of the Mini-Physical Interface Module (Mini-PIM) is enabled and configured as a trunk. [PR1076843](#)
- If the **flexible-vlan-tagging** option is configured on an underlying interface of a PPPoE interface (the logical interface), the **native-vlan** option is not supported. Traffic being sent out from the logical interface that has the **native-vlan** option configured will incorrectly contain the VLAN tag. [PR1084572](#)

Intrusion Detection and Prevention (IDP)

- On all SRX Series devices, the IDP exempt rule does not work when a source or destination zone is configured as a specific zone (instead of **any**), and if one or more IP addresses are configured to match the exempt rule and an attack traffic flow (destined to IP addresses that are configured to match the exempt rule) is for a standard application on a non-standard port (for example, HTTP ports other than 80). [PR1070331](#)
- On SRX Series devices with 2 GB of RAM, the maximum data segment size of the idpd process is limited to 200 million. Because of this limitation, the IDP policy compilation might fail. To avoid this issue, increase the maximum data segment size to 512 million. [PR1111946](#)

J-Web

- On SRX Series devices in a chassis cluster, you cannot set the password with special characters such as **!, @, #, \$, %, ^, ",** and so on using the J-Web chassis cluster wizard. [PR1084607](#)
- On all SRX Series devices, when you log in to J-Web using the logical system through Internet Explorer, the **Exception in data refresh** error might be displayed in the J-Web Dashboard messages log. [PR1096551](#)
- On all SRX Series devices, changing other ALG configuration through J-Web causes IKE-ESG ALG configuration to be changed. [PR1104346](#)

- On all SRX Series devices in J-Web, the **default** option under **Security > Logging > Application Tracking** is enabled. This setting enables application tracking if any system log configuration is saved. [PR1106629](#)
- On SRX Series devices, when a logical system (LSYS) user logs in to J-Web, changes the configuration, and clicks the Compare button, the result window does not pop up. [PR1115191](#)

Network Address Translation (NAT)

- On SRX Series devices in a chassis cluster, the H.323 ALG might not work properly after the chassis cluster failover. This is because the ALG binding synchronization message fails to synchronize the secondary device. [PR1082934](#)
- On all SRX Series devices, when the NAT configuration changes are made, the flowd process might stop. As a result, the memory allocation is affected. [PR1084907](#)
- On all SRX Series devices, the entry's timeout value of ALG is configured larger than the timer wheel's maximum timeout value (7200 seconds). However, this entry cannot be inserted into the timer wheel. As a result, an ALG persistent NAT binding leak occurs. [PR1088539](#)
- On all SRX Series devices, when domain names are used as a matching condition on security policies, the device sends the resolved request to the DNS server. If the DNS server is not reachable, the device tries to re-send the request to the DNS server. As a result, all the file descriptors on the nsd process become exhausted. [PR1089730](#)

Network Management and Monitoring

- On all SRX Series devices, when using point-to-multipoint (P2MP) automatic NHTB IPsec tunnels, routes using next hop IP that is in the st0.x subnet are incorrectly marked as active prior to the VPN tunnel establishment. [PR1042462](#)
- On SRX Series devices in a chassis cluster, when you reboot the primary node using the **request system reboot** command, the secondary node might stop after a few seconds. [PR1077626](#)

Platform and Infrastructure

- On all SRX Series devices, the oid ifSpeed of interface which is polled by SNMP is displayed incorrectly when the speed is configured as auto-negotiated. [PR967369](#)
- On SRX550 and SRX650 devices, 20 to 40 percent traffic loss is seen on the port of the SRX-GP-2XE-SFP-PTX after changing the speed from 10 GB to 1 GB. This issue is seen in both fiber and copper mode. When you switch between fiber and copper mode on the port of the SRX-GP-2XE-SFP-PTX, the speed might vary within the configuration. [PR1033369](#)
- On all SRX Series devices, the secondary node in a chassis cluster environment might stop or go into DB mode, displaying the **panic:rn timer_index_alloc** message. This issue is sometimes observed in a chassis

cluster environment with multipoint st0.x interface configured, and the tunnel interfaces flaps according to IPsec **idle-timeout** or IPsec **vpn-monitor**. [PR1035779](#)

- On SRX240 devices, after a system reboot, the link state of a VLAN interface might go down. [PR1041761](#)
- On SRX5400, SRX5600, and SRX5800 devices, an ICMP out error message is generated at the rate of 10,000 per second when you run the **show snmp mib get decimal 1.3.6.1.2.1.5.15.0** command. [PR1063472](#)
- A new version of boot loader (u-boot version 2.8) is included in the Junos OS. This new u-boot version contains a fix specifically for SRX210 HE2 devices that prevents the device from failing to boot in case of flash corruption. Note that the new u-boot will not be automatically installed but will be available for upgrade, which can be confirmed by using the **show system firmware** command. [PR1071560](#)
- On SRX1400, SRX3400, and SRX3600 devices in a chassis cluster, traffic fails to flow between logical systems (LSYS) when the secondary node goes offline. [PR1073068](#)
- In the scenario of MPLS over GRE, the MPLS traffic might fail to pass through the GRE tunnel after a system reboot. [PR1073733](#)
- On all SRX Series devices, when you use UTF-8 encoding to generate the certificate with the certificate authority (CA), certificate validation fails. [PR1079429](#)
- On SRX1400 devices with jumbo frames and low interpacket gaps, the interface (ge-0/0/0 to ge-0/0/5) reports Jabber or code violation errors, resulting in traffic loss. [PR1080191](#)
- On SRX550 and SRX650 devices, if a port of an 8-Port Gigabit Ethernet SFP XPIM card is set to the Ethernet switching family, locally generated packets might be dropped by the port. [PR1082040](#)
- If the destination interface and the next hop are configured for HTTP probes for real-time performance monitoring, the HTTP probes might not work. [PR1086142](#)
- On all SRX Series devices, the system log utility of the rtlogd process might stop when the WebTrends Enhanced Log File (WELF) format is configured for the security log. [PR1086738](#)
- The setting of Real-time Performance Monitoring (RPM) next hop metric value does not take effect. [PR1087753](#)
- On all SRX Series devices, the kernel might stop when running the automatic script. [PR1090549](#)
- On all SRX Series devices, the OpenSSL project has published a set of security advisories for vulnerabilities resolved in the OpenSSL library. Junos OS is affected by one or more of these vulnerabilities. Refer to JSA10694 for more information. [PR1095604](#)
- Upgrade to certain Junos OS versions might fail when a commit script is configured. [PR1096576](#)
- A syntax error is displayed when some unsupported commands are executed and when these commands are a part of the request support information as well. [PR1101846](#)
- An SPU might become inaccessible from the Routing Engine because of a memory-buffer counter corruption. Because of this issue, a service outage occurs in certain scenarios, for example, when IPsec is configured with certificate-based authentication. [PR1102376](#)

- When any of the two possible power supplies (PS) is missing on the SRX650 device, it does not generate the alarm. In addition, the device is checking if any of the two power supplies is functioning correctly to provide the result in the output of the **show chassis craft-interface** command. However, for the status of the power supply, the output of the **show chassis craft-interface** is **PS 0** instead of **PS**. [PR1104842](#)
- Starting in Junos OS Release 12.3X48-D20, the **set chassis fpc num sampling-instance name** command is required for J-Flow version 9 configuration. However, the commit fails when the **set chassis fpc num sampling-instance name** command is configured. [PR1108371](#)
- You cannot configure more than one lt-0/0/0.x interface per logical systems (LSYS) on the following Junos OS maintenance releases:

12.1X44-D35 through 12.1X44-D55

12.1X46-D25 through 12.1X46-D40

12.1X47-D10 through 12.1X47-D25

12.3X48-D10 through 12.3X48-D15

You can configure more than one lt-0/0/0.x interface per LSYS if you have no interconnect LSYS configured. If the interconnect LSYS is configured, then you can have only one lt-0/0/0.x interface per LSYS. The issue is fixed in the following Junos OS maintenance releases: 12.1X44-D60, 12.1X46-D45, 12.1X47-D30, and 12.3X48-D20. .

[PR1121888](#)

Routing Policy and Firewall Filters

- On SRX Series devices, the pre-defined application-sets can only be invoked in root Logical System (LSYS) and it cannot be invoked in custom LSYSs. [PR1075409](#)
- On all SRX Series devices, the security policy scheduler fails to activate or deactivate policies when the daylight saving time (DST) change occurs. [PR1080591](#)

Routing Protocols

- On all SRX Series devices, If the device acts as a rendezvous point (RP) in a multicast environment and if the interface of the RP is configured in a custom logical system (LSYS) or routing instance, then the register-stop messages might be incorrectly sent out from the root LSYS or routing instance instead of from the custom LSYS or routing instance. [PR1062305](#)

Unified Threat Management (UTM)

- On all SRX Series devices with secure wire and enhanced Web filtering configured, when the enhanced Web filtering initiates a session to the Websense server to validate the incoming request's category and if the request (the request to the Websense server) is transmitted in layer 3 mode first and then looped back to Layer 2 mode and forwarded out of the device, then this session (the session from the device to the Websense server) will not be established. This situation occurs because the reply from the Websense server only matches the session created in Layer 2 mode and does not match the session created in Layer 3 mode. [PR1090622](#)

User Interface and Configuration

- On all SRX Series devices, the packet capture function cannot be displayed through J-Web. However, the packet capture function can be disabled by using the CLI. [PR1023944](#)
- On all SRX Series devices, when you commit the traffic selector (TS) configuration, it might fail and an ffp core file might be generated. [PR1089676](#)

VPNs

- On SRX1400 devices, packets that are forwarded through the port of the SRX1K-SYSIO-GE card might be dropped due to CRC error. [PR1036166](#)
- On all SRX Series devices, the default trusted-ca list (Trusted_CAs.pem) is not supported by Junos OS. [PR1044944](#)
- On SRX Series devices with dynamic VPN configured, the KMD process restarts or stops, causing an IP address leak on the dynamic VPN address pool. [PR1063085](#)
- On SRX Series devices with IPsec VPN configured, the IPsec VPN tunnel might fail to reestablish after recovery tunnel flapping. This is because an old, invalid tunnel session exists on the central point. As a result, an attempt to create the new tunnel session fails. [PR1070991](#)
- On all SRX Series devices, the maximum number of characters allowed for an IKE policy name is limited to 31 bytes. Although you can configure more than 31 bytes by using the CLI, the bytes in excess of the limit are ignored on the data plane. [PR1072958](#)

- On all SRX Series devices with site-to-site IPsec VPN configured using IKEv2, if an active tunnel existed and the SRX Series device acted as the responder of IKEv2 negotiation, then the VPN peer initiating a duplicate IKEv2 Phase 2 negotiation request will cause the IPsec VPN tunnel to go to inactive state on the data plane side of the SRX Series device. [PR1074418](#)
- On SRX Series devices with dynamic VPN configured, the key management process (KMD) might stop when an IKE payload with a different port number is received. [PR1080326](#)
- On SRX Series devices with IPsec VPN configured, if the SRX Series device is the initiator and the other peer is from another vendors, the Internet Key Exchange (IKE) tunnel negotiation might not come up under certain conditions. [PR1085657](#)
- On SRX Series devices, when the **alarm-without-drop** option is configured for the UDP Flood Protection screen, packets classified as attack packets might be sent out of order. This can result in performance degradation. [PR1090963](#)
- On SRX Series devices, the output of the **show system processes resource-limits process-name pki-service** command cannot be shown correctly because of a missing file. [PR1091233](#)
- On SRX Series devices, in group VPN setups, memory might leak during the gksd and gkmd processes. [PR1098704](#)
- On SRX Series devices, an IPsec VPN using ESP encapsulation above the group VPN is not supported. As a result, the IPsec VPN traffic will be dropped because bad SPI packets are seen in the group VPN. [PR1102816](#)
- On all SRX Series devices, the IPsec tunnel does not come up on the data plane if both the st0 interface and the IPsec VPN configuration (which is configured in the **[security ike]** and **[security ipsec]** hierarchies) are committed in a single commit. [PR1104466](#)
- On all SRX Series devices, if redundant VPN tunnels are set up to use two different external interfaces within two different IKE gateways to connect the same VPN peer, and the RPM is configured for route failover and the VPN monitoring is configured when the primary link is down, then VPN fails to the secondary link as expected. However, when the primary link is up, VPN flapping might occur and establishment of the primary VPN tunnel might be delayed. [PR1109372](#)

Resolved Issues: Release 12.3X48-D15

Application Identification

- On all SRX series devices, when next-generation application identification is enabled and traffic is processed, intermittent high CPU utilization on data plane is observed. [PR1064680](#)

Application Layer Gateways (ALGs)

- On all SRX Series devices in a chassis cluster, with the TCP-based ALG enabled, if the TCP keepalive mechanism is used on the TCP server and client, after a data plane Redundancy Group (RG1+) failover, the keepalive message causes the mbuf to be held by ALG until the session timeout. This results in generation of a high mbuf usage alarm. Application communication failure occurs due to lack of mbuf. [PR1031910](#)
- On all SRX Series devices, if the SUN RPC traffic has the same IP address, port number, and program ID but is coming from different source zones other than the session, the traffic is dropped by the SUN RPC ALG. [PR1050339](#)
- On all SRX Series devices, the current SIP parser does not parse the quotation marks in the mime boundary, and the message body of the SIP messages might be cut off. [PR1064869](#)
- On all SRX Series devices with the MS-RPC ALG enabled, the flowd process might stop due to incorrect MS-RPC ALG parsing for the **ISystemActivator RemoteCreateInstance Response** packets. [PR1066697](#)

Chassis Cluster

- On all SRX Series devices in a chassis cluster, if the SCCP ALG enabled, the SCCP state flag might not be set properly while processing the SCCP call on the device. A related real-time object (RTO) hot synchronization might cause the flowd process to stop. [PR1034722](#)
- On SRX Series devices in a chassis cluster, the **count** option in the security policy might stop working after failover. This is because the Packet Forwarding Engine does not resend the message with policy states to the Routing Engine after failover. The policy lookup counter disappears when you run the **show security policies from-zone * to-zone * policy-name * detail |grep lookups** command. [PR1063654](#)
- On SRX Series devices in a chassis cluster, if the switching fabric (swfab) interface is configured, the swfab interface incorrectly updates the state of the fabric (fab) interface. As a result, the fab interface might hang in the down state. [PR1064005](#)

CLI

- On all SRX Series devices, the output of the **show interfaces detail** and **show interfaces extensive** CLI commands for the SHDSL interface in EFM mode might not be displayed. [PR1051641](#)

Dynamic Host Configuration Protocol (DHCP)

- In DHCP requests, the IP TTL value is set to 1 and the DHCP option 12 is missing. [PR1011406](#)
- On SRX Series devices configured as a DHCP server (using JDHCP), even though the next-server (siaddr) and tftp boot-server options are configured, the siaddr and tftp boot servers are set with the IP address as 0.0.0.0 in DHCP reply packets. [PR1034735](#)
- On all SRX Series devices, when an interface is configured as a DHCP client using the dhcpd process, if a hostname is not configured, the DHCP discover message will not be sent out and the DHCP client interface cannot fetch the IP address. [PR1073443](#)

Flow-Based and Packet-Based Processing

- On SRX5400, SRX5600, and SRX5800 devices with an IOC2 (SRX5K-MPC), configuring a sampling feature (flow monitoring) might cause high kernel heap memory usage. [PR1033359](#)
- On SRX Series devices, after IDP drop action is performed on a TCP session, the TCP session timeout is not accurate. [PR1052744](#)
- On SRX Series devices with IP-in-IP tunnel configured, due to incorrect configuration (routing loop caused by route change and so on), packets might be encapsulated by the IP-in-IP tunnel several times. As a result, packets are corrupted and the flowd process might stop. [PR1055492](#)
- On SRX240, SRX550, SRX650, SRX1400, SRX3400, SRX3600, SRX5400, SRX5600, and SRX5800 devices, in a rare condition, the session might be doubly released by multiple threads during internal processing by the NAT module. As a result, the flowd process to stop. [PR1058711](#)
- On all SRX Series devices, under certain race conditions, if the interface associated with the name server is down, the flowd process might stop because UTM internal function was not configured. [PR1066510](#)
- On SRX100 devices, when the device is configured as an authentication enforcer of 802.1x, authentication from certain special supplicants might fail. This is because the software engine that processes the next hops in the device incorrectly processes the packet coming from the supplicant with a special source MAC address. As a result, the packets are dropped. [PR1067588](#)
- On all SRX Series devices, when you run the **show security policies hit-count** command, the Routing Engine memory is overwritten, resulting in an nsd process to stop. This issue occurs when security policies are not synchronized between the Routing Engine and the data plane. [PR1069371](#)

General Packet Radio Service (GPRS)

- On SRX Series devices in a mobile packet core network, with GTPv2 enabled and the device configured as a border gateway, the GTP packets might be dropped with a missing information element drop reason message. The packets are dropped because the information element check in processing the GTPv2 modify bearer request is not accurate. The check should only exist when Tracking Area Updates (TAU), Routing Area Updates (RAU), or handover are processed with a Serving Gateway (SGW) change on the S5/8 interface. [PR1065958](#)

Interfaces and Routing

- On all SRX Series devices, if there are multiple logical interfaces configured under a physical interface, the **shaping-rate** percentage configured for queue under schedulers might improperly calculate the value based on the speed of the physical interface. [PR984052](#)
- On SRX100H2, SRX110H2, SRX210H2, SRX220H2 and SRX240H2 devices, when you enable VLAN tagging on interfaces and commit the configuration, the interface speed and duplex mode might cause the interface to stop processing traffic. [PR1003423](#)
- On all SRX Series devices, the **commit synchronize** command fails because the kernel socket might hang. [PR1027898](#)
- On SRX Series devices, in each node, there is only one Routing Engine. The Routing Engine 0 in the master node is the master Routing Engine and the RE 0 in the secondary node is the backup Routing Engine. The request system power-off both-routing-engines command powers off both the master and the backup Routing Engines simultaneously. [PR1039758](#)
- On SRX Series devices with PPPoE configured, when PPPoE fails to authenticate, the software next hop entry will leak in the data plane, gradually consuming all 64,000 software next hop entries. When the software next hop table is full, the following next hop error pops up: **RT_PFE: NH IPC op 2 (CHANGE NEXTHOP) failed, err 6 (No Memory) peer_class 0, peer_index 0 peer_type 10**. [PR1055882](#)
- On SRX Series devices, when the **set system autoinstallation interfaces interface-name bootp** command is configured, the autoinstallation enabled interface receives an IP address from the DHCP server and installs a default route on the data plane. If the autoinstallation enabled interface flaps, the default route might change and remain in dead state. [PR1065754](#)

Intrusion Detection and Prevention (IDP)

- On SRX devices, severity for the IDP report changes from log severity to threat severity. [PR1019401](#)

J-Web

- On SRX Series devices, when you use a configuration encryption, the missing rescue configuration alarm is set even when there is a saved rescue configuration. [PR1057473](#)
- On SRX Series devices, when you configure J-Web setup wizard through creating new configuration and applying the same does not reflect all the configurations in a router. This displays configuration change alert and ask for committing the configuration. [PR1058434](#)
- On all SRX Series devices, if a security policy contains a tcp-options statement, modifying this security policy by using J-Web results in the loss of the tcp-options statement. This is because the tcp-options configuration is missing in the J-Web security policy configuration. [PR1063593](#)

Network Address Translation (NAT)

- On SRX5400, SRX5600, and SRX5800 devices with the SPC2 (SRX5K-SPC-4-15-320) installed, if a NAT IP address pool is configured with a large number of IP addresses (more than 56, 000), then running the `show snmp mib walk jnxJsNatSrcNumPortInuse` command causes the LACP to flap. [PR1053650](#)

Security Policies

- On all SRX Series devices, if two security policies are combined such that the whole address space is used, then the secondary security policy might fail to evaluate the traffic. [PR1052426](#)

System Logging

- On all SRX Series devices, the `flowd_octeon_hm: pconn_client_connect: Failed to connect to the server after 0 retries` message repeats in the log. [PR1035936](#)
- On all SRX Series devices, when IDP IP action log is configured for a security policy that matches a user identification, the information of the user name and roles is not updated in IP action logs. [PR1055075](#)
- On all SRX Series devices, the user or role retrieval information is not updated properly in the structured syslog format. [PR1055097](#)
- On SRX100 devices, when you run the `show snmp mib walk jnxMibs` command, the chassisd log repeatedly generates the `fru is present: out of range slot -1 for FAN` message. [PR1062406](#)
- On SRX Series devices, the log displays the message `log: /kernel: veriexec: fingerprint for dev`. This is a cosmetic issue. [PR1064166](#)

Unified Threat Management (UTM)

- On SRX Series devices, due to a memory leak issue in the utmd process, the utmd process might cause control plane CPU utilization that is higher than expected even when the Unified Threat Management (UTM) feature is not enabled. The memory leak can only be triggered if there is a UTM license installed on the system. [PR1027986](#)
- On all SRX Series devices running Junos OS Release 12.3X48-D10 or later, with enhanced Web filtering configured, the connection to the Websense Threat Seeker Intelligence Cloud will time out if **strict-syn-check** is enabled under **security flow tcp-session** hierarchy. [PR1061064](#)

VPNs

- On SRX Series devices with IPsec VPN configuration, because of a rare timing issue, the IPsec VPN traffic might be dropped due to a "bad SPI" message on the traffic-receiving side during IPsec Security Association (SA) rekey. [PR1031890](#)
- On SRX Series devices with policy-based IPsec VPN configured, deleting security policies that are associated with a VPN tunnel might result in a stale VPN tunnel remaining. In addition, the stale VPN tunnel might be associated with the newly added security policies. [PR1034049](#)
- On SRX series devices, in a tunnel over route-based IPsec VPN, GRE or IP-in-IP tunnel scenario, such as IPsec VPN over GRE tunnel, after the encapsulation of the first tunnel, the next hop in internal processing might not be set properly to point to the second tunnel, which results in packet loss. [PR1051541](#)

Resolved Issues: Release 12.3X48-D10

Application Layer Gateways (ALGs)

- On all SRX Series devices with the SIP ALG and NAT enabled, if you place a call on hold or off hold many times, each time with different media ports, the resource in the call is used, resulting in one-way audio. Tearing down the call clears the resource, and following calls are not affected. [PR1032528](#)
- On all SRX Series devices with MSRPC ALG enabled, the flowd process might stop when ALG processes the MSRPC traffic which contains invalid Class IDs (CLSIDs) and unknown interface IDs (IIDs). [PR1036574](#)
- On all SRX Series devices with the SIP ALG and NAT enabled, the SIP ALG does not execute IP translation for the retransmitted 183 session progress messages. In this scenario, the SIP call will fail when the device receives the first 183 session progress messages without SDP information, but the retransmitted 183 session progress messages contains SDP information. [PR1036650](#)

- On all SRX Series devices, the DNS ALG does not terminate the session when a truncated DNS reply is received, so the session remains active until high timeout of 10~50 is reached. [PR1038800](#)
- On SRX Series devices, SIP ALG code has been enhanced to support RFC 4566 regarding the SDP lines order and to avoid issues of no NAT in owner field (O line) in some circumstances. [PR1049469](#)

Chassis Cluster

- On SRX5400, SRX5600, and SRX5800 devices with SPC2 (SRX5K-SPC-4-15-320) cards installed, when IP spoofing is enabled, after the device under test (DUT) is rebooted, the address books in the Packet Forwarding Engine will be removed and not pushed back into the Packet Forwarding Engine. Due to this issue, IP spoofing does not work after the reboot. [PR1025203](#)
- On SRX Series devices in chassis cluster Z mode (except SRX110 device), if static NAT or destination NAT is configured, and in the NAT rule the IP address of the **incoming interface** is used as a matching condition for the **destination-address**, then the traffic matching the NAT rule is discarded. [PR1040185](#)
- On SRX Series devices in a chassis cluster when the mbuf usage is more than 80 percent, the device will automatically fail over. To avoid UTM traffic-overwhelmed system mbuf usage on the device, UTM function will be not enabled on the new session when system buf usage is as high as 75 percent. When usage is down, UTM function could still continue to run on the new session. [PR1035986](#)
- On all SRX Series devices in a chassis cluster, during control plane RGO failover, a policy resynchronization operation compares the policy message between the Routing Engine and the Packet Forwarding Engine. However, some fields in the security policy data message are not processed. Data for unprocessed fields might be treated differently and cause the flowd process to stop. [PR1040819](#)

CLI

- On all SRX Series devices, the configurations of group junos-defaults are lost after a configuration rollback. As a result, the **commit** command fails. [PR1052925](#)

Dynamic Host Configuration Protocol (DHCP)

- On all SRX Series devices configured as a DHCP server (using the `jdhcpd` process), when the DHCP server gets a new request from a client and applies an IP address from the authentication process (`authd`), the `jdhcpd` process communicates with `authd` twice as expected (once for the DHCP discovery message and once for the DHCP request message). If the authentication fails in the first message, the `authd` process will indefinitely wait for the second authentication request. However, the `jdhcpd` process never sends the second request, because the process detects that the first authentication did not occur. This causes memory leak on the `authd` process, and the memory might get exhausted, generating a core file and preventing DHCP server service. High CPU usage on the Routing Engine might also be observed. [PR1042818](#)

Flow-Based and Packet-Based Processing

- On all SRX Series devices, after a failover, there is a reroute process for each existing session on the newly active device. The reroute is delayed and is triggered by the first packet hitting an existing session. If multiple packets of the same session come in at once, and are picked up by different threads for processing, only one thread will run the reroute, while the other threads have to wait for the result before forwarding the packet. This waiting period penalizes traffic for other sessions and affects the overall throughput. Therefore, such packets will be dropped instead of waiting in order to optimize the overall system fairness and throughput. This drop does not affect newly created sessions, because that is a different data path. [PR890785](#)
- On all SRX Series devices, when composite next hop is used, RSVP session flap might cause an ifstate mismatch between the master Routing Engine and the backup Routing Engine, leading to a kernel stop on the master Routing Engine. [PR905317](#)
- On all SRX Series devices, when you configure **http-get** RPM probes to measure the website response, the probes might fail because the HTTP server might incorrectly interpret the request coming from the device. [PR1001813](#)
- On SRX Series devices, I2C bus might hang due to read and write error with the same mutex and the following alarm message is displayed:

2014-06-26 00:18:23 SAST Major SRXSME Chassis Fan Tray Failure

2014-06-26 00:17:46 SAST Minor PEM 1 Absent

2014-06-26 00:17:46 SAST Minor PEM 0 Absent

[PR1006074](#)

- On SRX Series devices, the USB modem link goes down if you configure the init-command-string \n to \ and n 2 characters. [PR1020559](#)
- On all multiple thread-based SRX Series devices (SRX240 and above), if IDP, AppSecure, ALG, GTP, or the SCTP feature, which is required for serialization flow processing is enabled, the device might encounter an issue where two flow threads work on the same session at the same time for the serialization flow processing. This issue might cause memory corruption, and then result in a flowd process to stop. [PR1026692](#)
- On SRX Series devices, when you forward traffic, a flowd core file is generated. [PR1027306](#)
- On SRX Series devices, when you enable **flexible-vlan-tagging**, the return traffic might be dropped on the tagged interface with the following message: **packet dropped, pak dropped due to invalid I2 broadcast/multicast addr**". [PR1034602](#)
- On all SRX Series devices, when WebTrends Enhanced Log File (WELF) format is configured for the security log, the device generates very long WELF-formatted logs (for example, logs more than 1000 bytes). When the log is truncated on the Packet Forwarding Engine and sent to the Routing Engine, memory corruption occurs, causing the flowd process to stop. This issue generally occurs when UTM Web filtering is configured. [PR1038319](#)
- On all SRX Series devices, when a primary IP address of an interface changes, some IPsec tunnels terminated on that interface might go down. [PR1044620](#)

Hardware

- On SRX Series devices, the message **twsi0: Device timeout on unit 1** fills the console on soft reboot. [PR1050215](#)

Installation and Upgrade

- On SRX650 devices, if the u-boot revision is 2.5 or later, installing the Junos OS release image from TFTP in loader mode fails. [PR1016954](#)
- On SRX Series devices, AES-GCM is not compatible with previous Junos OS releases. After you upgrade the Junos OS release on the VPN node (SRX Series device), the VPN tunnel that uses AES-GCM for encryption might not reboot. [PR1037432](#)

Interfaces and Routing

- On SRX Series devices configured as a CHAP authentication client, in a PPPoE over ATM LLC encapsulation scenario, the connection might not be established because of an incorrect sequence of messages being exchanged with the second LNS. [PR1027305](#)
- On SRX210 and SRX220 devices, broadcast packets might not be sent to the Routing Engine after system initialization. [PR1029424](#)
- On all SRX Series devices, PIM register messages are not sent from the outgoing interface because the wrong outgoing interface is selected during route lookup. [PR1031185](#)
- On SRX1400, SRX3400, and SRX3600 devices, memory leak occurs on the Control Plane Processor (CPP) logical interfaces are deleted and the interprocess communication messages are received by the CPP. High memory usage on the CPP might be seen in an interface flapping situation. [PR1059127](#)

J-Web

- On SRX Series devices, J-Web sets a limitation on the size of the configuration fetched from a device to avoid memory exhaustion. When the configuration size exceeds this limitation, J-Web fails to load the configuration on Junos OS Release 12.3X48-D10. [PR1037073](#)
- On SRX Series devices, security policy log or security policy count is not displayed when the match condition is `RT_FLOW_SESSION`. [PR1056947](#)

Layer 2 Transparent Mode

- On all SRX Series devices in Layer 2 transparent mode, the flowd process might generate a core file when two packets of the same connection are received in a short time before the flow session is created, and destination MAC address lookup succeeds for these two packets. [PR1025983](#)

Network Address Translation (NAT)

- On all SRX Series devices, when source NAT is configured, the ports are allocated randomly by default. In rare circumstances, the global random port table of source pools or interfaces becomes damaged by certain services or traffic. This damage can result in low-range ports being assigned a higher priority in sessions. Ports might be reused quickly, causing application access failure. [PR1006649](#)
- On all SRX Series devices, when persistent NAT is enabled, allocation of resource (port) for an incoming session failed. The session reference count for that binding increases constantly even if no more sessions are associated with it. This results in stale entries in the persistent NAT binding table, which causes persistent NAT table exhaustion. [PR1036020](#)

Security

- OpenSSL released a Security Advisory that included CVE-2014-3566 known as the "POODLE" vulnerability. The SSL protocol 3.0 (SSLv3) uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain clear text data through a padding oracle attack. OpenSSL is upgraded to support for SSL 3.0 fallback protection (TLS_FALLBACK_SCSV). Refer to JSA10656 for more information. [PR1033938](#)

System Logging

- On SRX Series devices, if the stream mode logging has incomplete configuration for multiple streams, after reboot the system might not send out stream logs to the properly configured streams. [PR988798](#)

Unified Threat Management (UTM)

- On all SRX Series devices, when UTM Sophos antivirus is enabled and a file that is not supported by Sophos antivirus is transferred through SMTP, the device might not be able to handle the last packet, and mail will be on hold. When packets are later sent on this session, the packet that was on hold will be handled by the device and the system will return to normal state. [PR1049506](#)
- The default action of Web filtering does not work as expected. [PR1365389](#)

VPNs

- On all SRX Series devices, a certificate-based IKEv2 tunnel cannot be set up if remote identity is configured as wildcard (*) for the IKE gateway. [PR968614](#)
- On SRX Series devices with IPsec VPN configured using IKEv1, the device can hold only two pairs of IPsec SA per tunnel. When the third IPsec SA rekey occurs, the oldest IPsec SA is deleted. Due to this mechanism, a looping of IPsec SA rekey might occur. For example, when a VPN peer contains incorrect configuration that has more than two proxy IDs matching only one proxy ID on a device, the rekey looping issue might cause the flowd process to stop on multiple thread-based SRX Series platforms (SRX240 devices and higher). [PR996429](#)
- On SRX Series devices, in group VPN setups, all the already registered members might suddenly disappear from the key server due to memory leak. [PR1023940](#)
- On SRX Series devices, when IPsec VPN is enabled using IKE version 2 and a distinguished name is used to verify the IKEv2 phase 1 remote identity, a remote peer initiates IKEv2 Phase 1 Security Association (SA) renegotiation (SRX Series devices work as responders), the new negotiated VPN tunnel might stay in "inactive" state on the data plane, causing IPsec VPN traffic loss. [PR1028949](#)

- On SRX Series devices in a Dynamic End Point (DEP) VPN scenario, the VPN tunnel might stay in down state after you change the user-at-hostname value. [PR1029687](#)
- On SRX Series devices, when you reboot the device in an AutoVPN configuration mode, the VPN tunnel does not come up and reports a private key error message. [PR1032840](#)

RELATED DOCUMENTATION

New and Changed Features 12
Changes in Behavior and Syntax 36
Known Behavior 37
Known Issues 40
Documentation Updates 107
Documentation Updates 107

Documentation Updates

This section lists the errata and changes in the software documentation.

IPsec VPN User Guide for Security Devices

- The traffic selector feature referred to as reverse route insertion (RRI) is now called auto route insertion (ARI). ARI is the automatic insertion of a static route based on the remote IP address configured in a traffic selector.

[See [Understanding Auto Route Insertion](#).]

Various Guides

- Some Junos OS user, reference, and configuration guides—for example, the [Junos Software Routing Protocols Configuration Guide](#), [Junos OS CLI User Guide](#), and [Junos OS System Basics Configuration Guide](#)—mistakenly do not indicate SRX Series device support in the “Supported Platforms” list and other related support information; however, many of those documented Junos OS features are supported on SRX Series devices. For full, confirmed support information about SRX Series devices, please refer to Feature Explorer at <https://pathfinder.juniper.net/feature-explorer/>.

System Logs

- In Junos OS System Log Reference Guide for Security Devices for Release 12.1X47-D10, the System Log Message for RT_FLOW_SESSION_CREATE is as follows:

session created **source-address/source-port->destination-address/destination-port service-name nat-source-address/nat-source-port->nat-destination-address/nat-destination-port src-nat-rule-name dst-nat-rule-name protocol-id policy-name source-zone-name destination-zone-name session-id-32 username(roles) packet-incoming-interface.**

The corrected System Log Message is:

session created **source-address/source-port->destination-address/destination-port service-name nat-source-address/nat-source-port->nat-destination-address/nat-destination-port src-nat-rule-type src-nat-rule-name dst-nat-rule-type dst-nat-rule-name protocol-id policy-name source-zone-name destination-zone-name session-id-32 username(roles) packet-incoming-interface application nested-application encrypted.**

RELATED DOCUMENTATION

[New and Changed Features](#) | 12

Changes in Behavior and Syntax | 36

Known Behavior | 37

Known Issues | 40

Resolved Issues | 43

Migration, Upgrade, and Downgrade Instructions | 110

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- Installation and Upgrade | 110
- Migrating Group VPN Servers and Members | 111
- Upgrading an AppSecure Device | 115
- Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 116

This section contains the procedure to upgrade Junos OS, and the upgrade and downgrade policies for Junos OS. Upgrading or downgrading Junos OS can take several hours, depending on the size and configuration of the network.

NOTE: Upgrading to Junos OS Release 12.1X47-D10 or later is not supported on the J Series devices or on the versions of the SRX100 and SRX200 lines with less than 2GB memory. If you attempt to upgrade one of these devices to Junos OS 12.1X47-D10 or later, installation will be aborted with the following error message:

ERROR: Unsupported platform <platform-name >for 12.1X47 and higher

For more information, refer to the Knowledge Base article at <https://kb.juniper.net/TSB16632>.

Installation and Upgrade

On SRX5000 line of devices with SRX5K RE-13-20 (the first generation Routing Engine), a software upgrade to Junos OS Release 12.3X48-D80 and higher releases might fail the pre-check due to insufficient space available on the compact flash. As a workaround, downgrade to Junos OS Release 12.3X48-D10 first and then upgrade to the target release or fresh install the target release using the USB install-media. For more information, see [TSB17655](#).

Migrating Group VPN Servers and Members

IN THIS SECTION

- [Migration Scenarios and Considerations | 111](#)
- [Migration Scenario 1 | 112](#)
- [Migration Scenario 2 | 113](#)
- [Migration Scenario 3 | 115](#)

Junos OS Release 12.3X48-D30 allows Group VPN members on SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, and SRX650 devices (also referred to as Group VPNv1 members) to interoperate with Group VPNv2 servers. This section describes the procedure for migrating Group VPNv1 members from interoperating with a Group VPNv1 server to interoperating with a Group VPNv2 server.

NOTE: This section assumes that you have a working network of a Group VPNv1 server and Group VPNv1 members.

Migration Scenarios and Considerations

There are three scenarios for migrating Group VPNv1 members to interoperate with a Group VPNv2 server. [Table 1 on page 111](#) describes considerations for each of these scenarios.

Table 1: Considerations for Group VPN Migration Scenarios

Considerations	Migration Scenario 1	Migration Scenario 2	Migration Scenario 3
	The Group VPNv1 and Group VPNv2 servers have different IKE gateway addresses. The same group ID is used.	The Group VPNv1 and Group VPNv2 servers have the same IKE gateway address. The same group ID is used.	The Group VPNv1 and Group VPNv2 servers have different IKE gateway addresses and use different group IDs.
Impact on traffic during migration:	There is traffic loss until all members move to the Group VPNv2 server.	There is no traffic loss.	There is no traffic loss.

Table 1: Considerations for Group VPN Migration Scenarios (*continued*)

Considerations	Migration Scenario 1	Migration Scenario 2	Migration Scenario 3
clear security group-vpn member ike security-association operational command performed on each member during migration:	Not required.	Required.	Not required.
Configuration change needed on Group VPNv1 members during migration to Group VPNv2 server:	Minimal configuration change.	Minimal configuration change.	More substantial configuration change, including new group ID.
Configuration change needed on Group VPNv1 members during rollback from Group VPNv2 server to Group VPNv1 server.	Required.	Not required.	Not required.

The steps for migrating Group VPNv1 members for each scenario is described in the following sections.

Migration Scenario 1

In this scenario, the Group VPNv1 server and Group VPNv2 server use different IKE gateway addresses. The same group ID is configured on the Group VPNv1 and Group VPNv2 servers.

1. Verify that all Group VPNv1 members support the Junos OS 12.3X48 releases.
2. Upgrade all Group VPNv1 members to run Junos OS Release 12.3X48-D30 or a later 12.3X48 maintenance release.
3. Configure the Group VPNv2 server with the Group VPNv1 configuration, including the same group ID, with the following exceptions:
 - The IKE authentication algorithm configured must be **sha-256**.
 - The IPsec authentication algorithm configured must be **hmac-sha-256-128**.
 - At the **[edit security group-vpn server group group-name]** hierarchy level, do not configure **anti-replay-time-window** and **server-member-communication**.

4. On each Group VPNv1 member, configure a new IKE proposal that uses the **sha-256** authentication algorithm instead of MD5 or SHA1. Bind this IKE proposal to the current IKE policy and commit this change.

NOTE: IKE proposals are configured with the same Diffie Hellman (DH) group when aggressive mode exchange is used. Group VPNv1 supports DH groups 1, 2, 5, and 14, while Group VPNv2 supports DH groups 14 and 24.

5. On each Group VPNv1 member, change the IKE gateway address from the Group VPNv1 server's address to the Group VPNv2 server's address. When this configuration change is committed, the device reinitiates a new session with the Group VPNv2 server and also receives new TEK keys. This means that the device is not able to communicate securely with another member until the member has migrated to the Group VPNv2 server and received new TEK keys.

To roll back to the Group VPNv1 server:

- On each Group VPNv1 member, change the IKE gateway address from the Group VPNv2 server's address to the Group VPNv1 server's address. When this configuration change is committed, the device reinitiates a new session with the Group VPNv1 server and also receives new TEK keys. This means that the device is not able to communicate securely with another member until the member has migrated to the Group VPNv1 server and received new TEK keys.

Migration Scenario 2

In this scenario, the Group VPNv1 and Group VPNv2 servers use the same IKE gateway address.

1. Verify that all Group VPNv1 members support the Junos OS 12.3X48 releases.
2. Upgrade all Group VPNv1 members to run Junos OS Release 12.3X48-D30 or a later 12.3X48 maintenance release.
3. Configure the Group VPNv2 server with the Group VPNv1 configuration, including the same group ID, with the following exceptions:
 - The IKE authentication algorithm configured must be **sha-256**.
 - The IPsec authentication algorithm configured must be **hmac-sha-256-128**.
 - At the `[edit security group-vpn server group group-name]` hierarchy level, do not configure **anti-replay-time-window** and **server-member-communication**.

4. On the Group VPNv2 server, bring down the server's interface before connecting the Group VPNv2 server to the same network segment as the Group VPNv1 server. Only one server can be active at a time.
5. On the Group VPNv1 server, disable antireplay and heartbeat in the server configuration. Group VPNv1 and Group VPNv2 use different methods of antireplay, and heartbeats are not supported on Group VPNv2 servers.
6. On the Group VPNv1 server, change the TEK lifetime for all groups to a higher value to avoid rekeys on Group VPNv1 members while the Group VPNv2 server is being activated. To do this, use the **set security group-vpn server ipsec proposal *proposal-name* lifetime-seconds** command. The recommended value is based on how much time it takes to activate the Group VPNv2 server and to clear the IKE SA on all Group VPNv1 members.
7. On each Group VPNv1 member, configure a new IKE proposal that uses the **sha-256** authentication algorithm instead of MD5 or SHA1. Add this IKE proposal to the current IKE policy and commit this change.

NOTE: IKE proposals are configured with the same Diffie Hellman (DH) group when aggressive mode exchange is used. Group VPNv1 supports DH groups 1, 2, 5, and 14, while Group VPNv2 supports DH groups 14 and 24.

8. On the Group VPNv1 server, bring down the server's interface to the network.
9. On the Group VPNv2 server, bring up the server's interface to the network.
10. On each Group VPNv1 member, clear the existing IKE SA so that a new IKE SA is used for the next **groupkey-pull** with the Group VPNv2 server. To do this, issue the **clear security group-vpn member ike security-associations** command on the member.

To roll back to the Group VPNv1 server:

1. Bring down the Group VPNv2 server's interface, then bring up the Group VPNv1 server's interface.
2. On each Group VPNv1 member, clear the existing IKE SA so that a new IKE SA is used for the next **groupkey-pull** with the Group VPNv1 server. To do this, issue the **clear security group-vpn member ike security-associations** command on the member.

Migration Scenario 3

In this scenario, the Group VPNv1 server and Group VPNv2 server use different IKE gateway addresses. A different group ID is configured on the Group VPNv1 and Group VPNv2 servers.

1. Verify that all Group VPNv1 members support the Junos OS 12.3X48 releases.
2. Upgrade all Group VPNv1 members to run Junos OS 12.3X48-D30 or a later 12.3X48 maintenance release.
3. Configure the Group VPNv2 server with the Group VPNv1 configuration, with the following exceptions:
 - The IKE authentication algorithm configured must be **sha-256**.
 - The IPsec authentication algorithm configured must be **hmac-sha-256-128**.
 - At the **[edit security group-vpn server group group-name]** hierarchy level, do not configure **anti-replay-time-window** and **server-member-communication**.
 - The group ID should be your preferred value.
4. On each Group VPNv1 member, configure a new IKE, IPsec group, and scope policy that matches the configuration on the Group VPNv2 server. When these changes are committed, the Group VPN v1 member will connect to the Group VPNv2 server and download new group policies and TEK keys from the Group VPNv2 server.

Upon expiration of the hard lifetime, the TEK keys downloaded from the Group VPNv1 server are deleted. Subsequent traffic uses the TEK keys downloaded from the Group VPNv2 server.

NOTE: The new scope policy that works with the Group VPNv2 server must remain below the scope policy that works with the Group VPNv1 server.

5. On the Group VPNv1 server, disable the interface that connects to the Group VPNv1 members.

To roll back to the Group VPNv1 server:

- First disable the interface on the Group VPNv2 server that connects to the Group VPNv1 members. Then enable the interface on the Group VPNv1 server that connects to the Group VPNv1 members.

Upgrading an AppSecure Device

Use the no-validate Option for AppSecure Devices.

For devices implementing AppSecure services, use the no-validate option when upgrading from Junos OS Release 11.2 or earlier to Junos OS 11.4R1 or later. The application signature package used with AppSecure services in previous releases has been moved from the configuration file to a signature database. This change in location can trigger an error during the validation step and interrupt the Junos OS upgrade. The no-validate option bypasses this step.

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases

Support for upgrades and downgrades that span more than three Junos OS releases at a time is not provided, except for releases that are designated as Extended End-of-Life (EEOL) releases. EEOL releases provide direct upgrade and downgrade paths—you can upgrade directly from one EEOL release to the next EEOL release even though EEOL releases generally occur in increments beyond three releases.

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 12.3X48, 15.1X49, 17.3 and 17.4 are EEOL releases. For example, you can upgrade from Junos OS Release 15.1X49 to Release 17.3 or from Junos OS Release 15.1X49 to Release 17.4. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind.

You cannot upgrade directly from a non-EEOL release to a release that is more than three releases ahead or behind. To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

For more information about EEOL releases and to review a list of EEOL releases, see <https://www.juniper.net/support/eol/junos.html>.

For information about software installation and upgrade, see the [Installation and Upgrade Guide for Security Devices](#).

For information about ISSU, see the [Chassis Cluster User Guide for Security Devices](#).

RELATED DOCUMENTATION

[New and Changed Features | 12](#)

[Changes in Behavior and Syntax | 36](#)

[Known Behavior | 37](#)

[Known Issues | 40](#)

[Resolved Issues | 43](#)

Product Compatibility

IN THIS SECTION

- [Hardware Compatibility | 117](#)
- [Transceiver Compatibility for SRX Series Devices | 117](#)

This section lists the product compatibility for any Junos OS SRX Series mainline or maintenance release.

Hardware Compatibility

To obtain information about the components that are supported on the device, and special compatibility guidelines with the release, see the SRX Series Hardware Guide.

To determine the features supported on SRX Series devices in this release, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at <https://pathfinder.juniper.net/feature-explorer/>.

Transceiver Compatibility for SRX Series Devices

We strongly recommend that only transceivers provided by Juniper Networks be used on SRX Series interface modules. Different transceiver types (long-range, short-range, copper, and others) can be used together on multiport SFP interface modules as long as they are provided by Juniper Networks. We cannot guarantee that the interface module will operate correctly if third-party transceivers are used.

Please contact Juniper Networks for the correct transceiver part number for your device.

Finding More Information

- **Feature Explorer**—Determine the features supported on MX Series, PTX Series, QFX Series devices. The Juniper Networks Feature Explorer is a Web-based app that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. <https://pathfinder.juniper.net/feature-explorer/>
- **PR Search Tool**—Keep track of the latest and additional information about Junos OS open defects and issues resolved. prsearch.juniper.net.
- **Hardware Compatibility Tool**—Determine optical interfaces and transceivers supported across all platforms. apps.juniper.net/hct/home

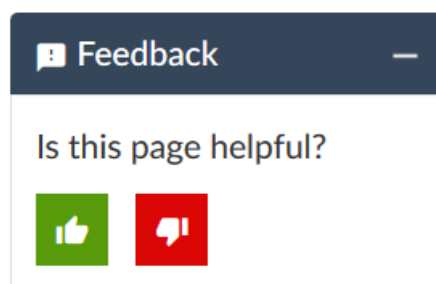
NOTE: To obtain information about the components that are supported on the devices, and the special compatibility guidelines with the release, see the Hardware Guide for the product.

- **Juniper Networks Compliance Advisor**—Review regulatory compliance information about [Common Criteria](#), [FIPS](#), [Homologation](#), [RoHS2](#), and [USGv6](#) for Juniper Networks products. apps.juniper.net/compliance/.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the [Juniper Networks TechLibrary](#) site, and do one of the following:



- Click the thumbs-up icon if the information on the page was helpful to you.

- Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post sales technical support, you can access our tools and resources online or open a case with JTAC.

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://support.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <https://support.juniper.net/support/>
- Search for known bugs: <https://kb.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://support.juniper.net/support/downloads/>

- Search technical bulletins for relevant hardware and software notifications:
<https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://forums.juniper.net>
- Open a case online in the CSC Case Management tool: <https://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool:
<https://entitlementsearch.juniper.net/entitlementsearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <https://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, visit us at
<https://support.juniper.net/support/requesting-support/>.

If you are reporting a hardware or software problem, issue the following command from the CLI before contacting support:

```
user@host> request support information | save filename
```

To provide a core file to Juniper Networks for analysis, compress the file with the **gzip** utility, rename the file to include your company name, and copy it to **ftp.juniper.net/pub/incoming**. Then send the filename, along with software version information (the output of the **show version** command) and the configuration, to support@juniper.net. For documentation issues, fill out the bug report form located at <https://www.juniper.net/documentation/feedback/>.

Revision History

4 August 2020—Revision 1— Junos OS 12.3X48-D105 – SRX Series.

Copyright © 2020 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.